NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

CIS

Congressional Information Service
Washington, D.C.

S. Hrg. 100-1078

HIGH-TECH TERRORISM

HEARINGS

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDREDTH CONGRESS

SECOND SESSION

ON

HIGH-TECH TERRORISM

MAY 19 AND SEPTEMBER 15, 1988

Serial No. J-100-68

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
20-146 WASHINGTON : 1989

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

S521-8

COMMITTEE ON THE JUDICIARY

JOSEPH R. BIDEN, Jr., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts
ROBERT C. BYRD, West Virginia
HOWARD M. METZENBAUM, Ohio
DENNIS DeCONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois

STROM THURMOND, South Carolina
ORRIN G. HATCH, Utah
ALAN K. SIMPSON, Wyoming
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
GORDON J. HUMPHREY, New Hampshire

Mark H. Gitenstein, *Chief Counsel*
Diana Huffman, *Staff Director*
Dennis W. Shedd, *Minority Chief Counsel*

Subcommittee on Technology and the Law

PATRICK J. LEAHY, Vermont, *Chairman*

DENNIS DeCONCINI, Arizona

GORDON J. HUMPHREY, New Hampshire

Ann M. Harkins, *Chief Counsel*
George C. Smith, *Minority Chief Counsel*

CONTENTS

Hearings held: Page
- Thursday, May 19, 1988 1
- Thursday, September 15, 1988 67

OPENING STATEMENT

Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 1, 67

CHRONOLOGICAL LIST OF WITNESSES

THURSDAY, MAY 19, 1988

Panel consisting of Oliver B. Revell, Executive Assistant Director of Investigation. Federal Bureau of Investigation; and L. Paul Bremer, Ambassador at Large for Counterterrorism, Department of State 3

Panel consisting of Robert H. Kupperman, senior associate, Center for Strategic and International Studies; and R. James Woolsey, Shea & Gardner 47

THURSDAY, SEPTEMBER 15, 1988

Panel consisting of Oliver B. Revell, Executive Assistant Director, Federal Bureau of Investigation; Edward V. Badolato, Deputy Assistant Secretary for Energy Emergencies, U.S. Department of Energy; George Woloshyn, Associate Director, National Preparedness Directorate, Federal Emergency Management Agency; and Craig Alderman, Jr., Deputy Under Secretary for Policy, Department of Defense 69

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Alderman, Craig, Jr.:
- Testimony 113
- Prepared statement 116

Badolato, Edward V.:
- Testimony 75
- Prepared statement 77

Bremer, L. Paul:
- Testimony 25
- Prepared statement 33

Kupperman, Robert H.:
- Testimony 47
- Prepared statement 51

Revell, Oliver B.:
- Testimony 3, 69
- Prepared statement 10, 71

Woloshyn, George:
- Testimony 102
- Prepared statement 104

Woolsey, R. James:
- Testimony 57
- Prepared statement 51

HIGH-TECH TERRORISM

THURSDAY, MAY 19, 1988

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:40 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Patrick Leahy (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator **LEAHY**. Good morning. This morning, the Technology and the Law Subcommittee will be hearing from several distinguished witnesses on the issue of technology and terrorism.

The subcommittee will first hear from Mr. Oliver Revell, the Executive Assistant Director of the Federal Bureau of Investigation. Mr. Revell, we are glad to see you here for the second time this week, I believe.

Mr. **REVELL**. Yes, sir.

Senator **LEAHY**. And Mr. L. Paul Bremer, the Ambassador at Large for Counterterrorism in the Department of State. Ambassador Bremer, it is good to have you here. They represent the lead agencies in dealing with the international and domestic terrorism menace.

Later, we will be talking with Dr. Robert Kupperman, a noted terrorism expert at the Center for Strategic and International Studies, and Mr. James Woolsey, of Shea and Gardner, a well-known expert in defense and security matters.

Now, this is a sensitive subject and the subcommittee intends to approach it with due caution, as this is an open hearing. I recognize that our executive branch witnesses will be restrained by classification, but I urge them to be as forthcoming as they can, consistent with protecting confidential information.

If there are areas of a classified nature, the subcommittee would consider a closed hearing at a later date and we, of course, would do that in one of the secure rooms of the Capitol.

Now, let me first outline what the subcommittee is interested in, and why. Thanks to the superb work of the FBI and State and local law enforcement, there have been few successful terrorist attacks upon the United States. International terrorism, which has attacked American interests abroad, has not come to our shores in any significant way.

The law enforcement agencies of the United States have constrained domestic terrorism, the home-grown violence perpetrated by hate groups. For this relative immunity, we should, and I think we can be thankful, but we cannot be complacent and assume it is never going to happen here.

Terrorism can, and I am afraid almost certainly will happen here. The United States is involved indirectly in conflicts in the Middle East, in Central America, in Southern Africa, and Asia. Many of these countries see America as an enemy of poor countries with small armies and few natural resources.

Some, like Libya, Iran, Syria, South Yemen, and Iraq, use terrorism to make up for economic and military shortcomings. They are never going to match us militarily, but they feel they can strike blows if they can do it through terrorism.

There is debate among experts on how terrorists will attempt to export their brand of fear and intimidation to this country. The weight of opinion seems to conclude that it is inevitable; that the infrastructure is already in place.

When terrorists strike, most experts believe they will make use of technology on two fronts. First, terrorists can use technology to carry out their attacks. We already have seen them use hard-to-detect plastic explosives, sophisticated communications equipment, precision-guided, hand-held missiles, automatic weapons, electronic surveillance gear, and miniature guns. We should expect terrorist operations here to employ more sophisticated methods. Ironically, some of this is due to the very effectiveness of our law enforcement efforts.

But more frightening, terrorists may try to do great harm, or at least threaten such harm, with nuclear, chemical or biological materials. Literature in the public domain shows how to manufacture a crude nuclear explosive device, how to culture biological agents of extraordinary lethality.

We have hundreds of undefended medical centers and research labs with radioactive substances and with biological agents. Deadly chemicals are readily available on the open market. Chemical weapons are already in the hands of several countries such as Iraq and Iran, and we have seen their use. They host or aid terrorist groups.

Now, the second way terrorists may exploit technology is by attacking the vulnerabilities of this, the most highly industrialized country in the world. The United States depends on an intricate web of computerized networks.

The smooth operation of electric and natural gas transmission systems, of uninterrupted electronic information transfer, of financial and business operations carried out over telephone lines, of a vast, complex transportation system that has many chokepoints—all of these systems are vital to our country.

A study by Dr. Kupperman and Mr. Woolsey entitled "America's Hidden Vulnerabilities" shows how frighteningly exposed we are to disruption by a handful of intelligent and determined terrorists. Most of what they need to carry out very feasible attacks on one of our great interlocking systems is readily available.

The purpose of this hearing today is to take a hard look at the connection between terrorism and technology. I want to get a sense of how real the present and future threat of high-tech terrorism is, how well we are prepared to deal with it, and what more we can and should be doing.

Now, as a nation, we spend hundreds of billions of dollars preparing to fight a nuclear war with the Soviet Union, probably the least likely of all the major threats to our national security. Nobody questions, nor do I, those kinds of expenditures.

But when it comes to high-tech terrorism, we are babes in the woods. Very little is spent, and I hope these hearings today will draw some attention to this real and present danger.

So, Mr. Revell and Ambassador Bremer, I welcome you. I have given an overly long opening statement, for me, anyway. But this is an area I have been concerned about for a long time; both when I was a prosecutor, and in the Senate as a member of the Judiciary Committee and as a member of the Intelligence Committee. The more I learn the more concerned I get.

So, Mr. Revell, it is over to you, sir.

PANEL CONSISTING OF OLIVER B. REVELL, EXECUTIVE ASSISTANT DIRECTOR OF INVESTIGATION, FEDERAL BUREAU OF INVESTIGATION; AND L. PAUL BREMER, AMBASSADOR AT LARGE FOR COUNTERTERRORISM, DEPARTMENT OF STATE

STATEMENT OF OLIVER B. REVELL

Mr. REVELL. Thank you, Mr. Chairman. It is good to be back for the second time this week.

Senator LEAHY. We are going to start having your mail forwarded here.

Mr. REVELL. Let me first make a little technical change, since my statement is being given out, my full statement. On page 14, we found an error in statistics and I want to make a correction that on the paragraph that says, "An analysis of terrorist incidents between 1983 to present reveals that," and the new statistic should be, "72 of the 84 incidents were actual or attempted bombings." So I put that on the record.

Mr. Chairman, we certainly share the concerns that you have expressed, and in my summary I would like to point out the highlights of what is in my full text where I believe that we do emphasize several of the same points.

As you indicated, the United States has not suffered terrorism at the same level of terrorist activities elsewhere in the world. We believe that there are sound reasons for the low incidence of terrorism in the United States.

In 1982, because of the threat of terrorism, the FBI established terrorism as a national priority on an equal status with counterintelligence, organized crime, and white collar crime, even though the number of incidents statistically would not have indicated that we should give it that level of priority.

Our counterterrorism program has been extremely successful. Between 1980 and 1982, there were an estimated 122 incidents in the United States. From that point, we have seen the numbers come down very drastically to the point where last year we had seven incidents and this year so far only two.

Now, that just did not happen; that was not happenstance. That did not come about through chance. That was through a very careful and controlled collection of intelligence, outstanding cooperation, and diligent investigation.

We and other law enforcement agencies have been able to prevent over the last 5 years 54 specific terrorist incidents that would have amounted to hundreds of casualties. If those incidents had occurred, then the United States would be known as a focal point for terrorism.

So, the fact that you do not see the incidents occurring does not mean that there are not groups or organizations that are bent upon committing acts of terrorism in the United States, as well as against the United States internationally.

In order to continue to prevent terrorism from occurring in the United States, it is absolutely essential that information of an intelligence nature be collected and carefully evaluated to determine its validity.

The FBI devotes considerable resources to the analysis of information acquired through its process of analysis and investigation. That information must be carefully vetted and prioritized.

Sometimes this information, and quite often, in fact, leads to the evidence for prosecution. We have seen a number of cases being prosecuted this year. However, not all intelligence leads to prosecution. Nevertheless, it does lead to actions on behalf of the Government or to actions that we can take to prevent incidents from occurring short of prosecution.

The principal goal of the FBI is to prevent terrorist acts from taking place. However, in the event that we are unable to prevent an incident from occurring, we have established comprehensive plans for responding to such incidents both here and abroad.

We have established 12 joint terrorism task forces in major cities of the United States. These task forces, which are made up of Federal, State, and local law enforcement officers, were established to deal with terrorism problems in specific areas and to facilitate the exchange of information and joint investigative activities.

This effort has been extremely successful in deterring criminal activity of terrorists, as well as solving criminal acts committed by terrorist groups after the fact. Just last week, the excellent work of the New York Joint Terrorism Task Force led to the convictions of Mutulu Shakur, a leader of the Republic of New Africa Group, and Marilyn Jean Buck, a member of the May 19 Communist Organization, for their participation in a 1981 robbery of an armored car and the murder of a Brink's guard and two police officers.

We call that the NYROB case, and it was that case that led us to the determination of a coalition between extreme left groups in the United States where they were aiding and abetting and supporting each other in a number of interrelated terrorist activities. They were also convicted of a number of other serious crimes and face penalties up to life imprisonment.

On the same day of these convictions, a Federal grand jury here in Washington indicted seven persons for the 1983 bombing of the U.S. Capitol and several other bombings of Government buildings.

By the way, I have been asked many times in appearances up here when we were going to solve that case. This is the first time I have had to testify since we have solved it, and so I would like to point out that we fulfilled our promise; we did solve it.

Senator **Leahy**. You did not have anybody up here that was watching that case, did you, Mr. Revell?

Mr. **Revell**. Not at all. There was not much interest up here.

Senator **Leahy**. None among the hundred Senators who had been standing nearby there just 2 hours before the explosion.

Mr. **Revell**. The gentleman who leads this body, whose office the explosion occurred next to, did exhibit some interest in that matter.

Senator **Leahy**. I have a feeling he might have.

Mr. **Revell**. One of those indicted was Marilyn Jean Buck, who has just been convicted in a New York case. Both the New York and Washington cases were the result of cooperative law enforcement efforts led by the FBI.

I would like to note that the individuals arrested and convicted are highly intelligent, and they constitute a very sophisticated terrorist group. They and others like them could have represented a threat to the infrastructure of the United States if not identified, arrested, and prosecuted.

Our projections for future terrorist activities in this country are based upon past experience, intelligence information gleaned through our investigations, informants and assets, information provided to us by other components of the U.S. Government, and by the law enforcement community and foreign governments.

Although the United States has not experienced an act of terrorism involving nuclear, chemical, biological, or other highly technical weapons, we have aggressively pursued the coordination of interagency operational responses to prepare for crises such as these.

Much of what we are doing and the initiatives we are taking cannot be discussed in this session, as you indicated. However, I would like to point out some of the things we are doing to prepare for these type incidents which would be the most difficult, obviously, for a free society to deal with.

Of particular concern to the FBI has been the threat of nuclear terrorism. The FBI has worked to establish a coordinated effort domestically for responding to threats of nuclear terrorism.

I should point out that we do not have an assessment that indicates that nuclear terrorism is at all likely. In fact, just the opposite. All the estimates and all the intelligence would indicate that this is an extremely remote possibility.

However, due to the dire circumstances that would be involved if there was even a semblance of a successful terrorist incident involving nuclear materials or nuclear devices, we expend extraordinary efforts to be prepared to respond to any such eventuality.

One of the most ambitious projects that we are currently working on is the establishment of a response for chemical and biological terrorism. The spread of chemical weapons in the Third World has increased the possibility that terrorists will acquire these weapons and the capability to use them. State-sponsored terrorism increases the potential for such an incident. The FBI has worked very hard to be prepared for this possibility and is working to develop an interagency response along with the IGT that Ambassador Bremer chairs.

Mr. Chairman, I know that one of your concerns is the vulnerability of the infrastructure, and I have had a number of conversations with one of your witnesses, Dr. Kupperman, about this potentiality.

Senator LEAHY. In fact, if I could interject there, Mr. Revell, some of the writings by Dr. Kupperman and Mr. Woolsey have concerned me a great deal; also, the Vice President's Report on Terrorism, where he says:

> Our vulnerability lies ironically in the strength of our open society and highly sophisticated infrastructure. Transportation, energy, communications, finance, and so on, are all interrelated Given these inherent vulnerabilities and the fact that Americans are increasingly the targets of terrorist attacks outside the United States, it is apparent that a potentially serious domestic threat exists.

At some point I want to go back to discuss the concern you mentioned about a nuclear threat and the steps we might take on that. But, first, what about this interconnected, interrelated, high-tech infrastructure that seems so vulnerable? What do we do about that?

Mr. REVELL. Well, Dr. Kupperman, of course, was a consultant to the Vice President's task force, and I was on the senior review group of the task force, so the task force did take cognizance of that potential.

In an open and free society where we are a very complex and sophisticated network of various supporting activities—rail transportation, communications, aviation, electronic funds transfer, gas and oil pipelines, sea lanes, and so forth—and we have seen certain natural phenomena tieup segments of our society, the New York black-outs, and so forth.

All you need to see is what happens when there is a wreck on a freeway or a bridge is in some way damaged to see the disruption that can occur. We certainly are cognizant of the fact that this society is vulnerable and that it is virtually unprotectable from the standpoint of security measures. You cannot establish in an open society a bunker mentality.

You had a debate here as to what sort of security precautions to take in the Capitol building. What type of access should the public have to their legislators? What type of security should you have? I think you made some reasonable adjustments, and yet preserved the openness of this particular facility. We have to do the same thing. We have to determine what are the most sensitive and the most important of these critical nodes that represent the support of our society, make sure that reasonable precautions are taken, make sure that we collect intelligence on those groups that are likely to carry out attacks of this nature and are in a position to prevent such acts, and then if we ultimately fail, be prepared to deal with the consequences, both the response of law enforcement and the support agencies such as FEMA and others that would come in to deal with the consequences. We are working in all of those areas.

Senator LEAHY. Well, let me follow on that just a little bit more because it is not just the terrible acts that might occur. I understand that terrorists could knock out major segments of networks, as long as they have the equipment and the money. We know that a number of the terrorist organizations have state support with very deep pockets, and get all the financial support they need.

They sometimes have diplomatic immunity so that they can move equipment in diplomatic pouches. They certainly have an ability to travel to any part of the world in a very short time.

So, on the one hand we have the threat of a major part of our telecommunications or electrical grids or natural gas lines being knocked out. But on the other hand we have the problem of extortion. To what extent can we be blackmailed by terrorists threatening such an incident—at the beginning of a summit meeting or at the time of major negotiations, for example, in the Middle East on a peace mission of some sort?

To what extent can the United States—which could never be defeated militarily by these groups—have its foreign policy and maybe even its economic policy thwarted by the threat of terrorist action?

Of course, the other problem we face from the threat of terrorist action here at home is whether there comes a point when the United States cut back its own constitutional safeguards—something none of our enemies in World War II or World War I were able to force us to do.

Basically, my question is this: What do you see as the most likely high-tech terrorism threat in the near future? As I understand your testimony, you have ruled out a nuclear threat, but what do you see as the greatest high-tech terrorist threat that we must be prepared to deal with?

Mr. **Revell**. If I was putting it on a scale of probabilities, I would say the most probable would be a chemical device that could be catastrophic, more so than a biological because biological devices are very difficult to obtain and very difficult to transport and very difficult to utilize.

Chemicals are available readily. Bhopal indicated how devastating they can be. You could even use a stand-off weapon and attack containers. You could use the transport, which is done both by rail and truck in this country, of very lethal chemicals.

So, if a terrorist group was going to escalate substantially—and in part of Ambassador Bremer's testimony he will cover some of those aspects—there does not seem to be any tendency to do that because they are very successful with what they are trying to do with the weapons at hand.

But if they were to decide, because of countermeasures and security measures and hardening of targets, that they wanted to ratchet up substantially the stakes involved, my view would be that the most amenable methods for them, the most likelihood they would have of success would be to go to the chemical device that could have, in a metropolitan area or a heavily populated area, a rather devastating impact if not dealt with very quickly.

Senator **Leahy**. Is it too much of a simplification to say the only real defense against something like that is intelligence and preemptive action to stop it from happening, because if they made such an attempt, there really is no way of defending?

Mr. **Revell**. In this society, as you know, everyone can obtain a weapon, they can travel freely, they can come in and out of the country virtually unfettered. Once in the country, as Mr. Yukikumura, they can travel around and pick up materials to build devices.

There is no way in our society to have sufficient security measures to prevent a terrorist from attacking a target of very high vulnerability and potential consequences, high consequences.

The only way that I know and the only way that I think that we have been successful to date is the very careful collection of intelligence and the use of that intelligence for preemptive action.

Now, preemptive action in this country is the use of law enforcement—arrests, searches, and seizures. Extremely effective; it does the job. It is not exotic, but it does prevent acts of terrorism.

A case in Chicago, the FALN—we were able through intelligence to place closed-circuit television inside two safehouses. We watched the terrorists building the bombs. We were able, then, by a court order to go in and disable those bombs, and also disable the automatic weapons.

As they proceeded out to go and bomb an Armed Forces Day parade and three military facilities, we arrested them. Well, that parade, if it had been bombed, could have caused mass casualties, and certainly the bombs going off at the armories could have.

So, the point is that the intelligence that we collected and used through arrests and searches was the precisely proper way for us in this society to deal with terrorism.

Senator **Leahy**. You really have to have it before the fact?

Mr. **Revell**. The only way that I think you can be successful is before the fact. Now, we are not always going to be successful.

Senator **Leahy**. I understand.

Mr. **Revell**. You cannot always prevent it, so we must be prepared to respond as well.

Senator **Leahy**. In my own State of Vermont, I noticed the U.S. attorney in papers he filed yesterday, an FBI affidavit, said that three men arrested in Richford, Vermont, are members of a Syrian terrorist organization responsible for the 1982 assassination of Lebanese president-elect, Bashir Gemayel.

I recall the day that happened the Secretary of State, Mr. Shultz, made it a point to mention to me how proud he was of the police chief in Richford, Vermont.

Mr. **Revell**. I mentioned it in my statement.

Senator **Leahy**. I know you did, and I appreciate that. I intend to make sure that the chief knows about that. In a rural area like that, had the chief not come along when he did, the terrorists could have gone much further. They were only a couple hundred miles from New York City.

Mr. **Revell**. Well, one of the things we are trying to do is—there are only 9,000 FBI agents. If you took all the Federal officers of all the agencies, you would not have a very significant force.

But we have 900,000 police officers out there, and they are in the rural areas, they are in the metropolitan areas, they are on the highways. If we can create a state of alertness and readiness and a knowledge as to how to deal with these incidents, such as the State trooper in New Jersey and the chief in Vermont, then we have a much more formidable defensive line out there operating within the constraints of our constitutional rights and privileges and in the everyday activities of law enforcement.

Yet, they do provide a very formidable defense against those elements who would carry out acts of terrorism.

[The statement of Mr. Revell follows:]

OPENING STATEMENT OF
OLIVER B. REVELL,
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

TERRORISM, AND THE VIOLENT CRIMINAL ACTS ASSOCIATED WITH TERRORIST INCIDENTS, CONTINUE TO PLAGUE MANY NATIONS OF THE WORLD. THE CURRENT STATE OF GLOBAL AFFAIRS MAKES ALL NATIONS SUSCEPTIBLE TO TERRORISM. ACCORDING TO RECENT STATISTICS COMPILED BY THE U.S. DEPARTMENT OF STATE, 832 INTERNATIONAL TERRORIST INCIDENTS OCCURRED WORLDWIDE DURING 1987. COMPARED TO THE 774 INCIDENTS IN 1986 AND 782 INCIDENTS IN 1985, THESE STATISTICS CLEARLY SHOW A CONTINUED HIGH LEVEL OF INTERNATIONAL TERRORIST VIOLENCE.

THE UNITED STATES HAS NOT EXPERIENCED ANYWHERE NEAR THESE HIGH LEVELS OF TERRORIST INCIDENTS. IN FACT, SINCE 1983 THERE HAS NOT BEEN A SUCCESSFUL TERRORIST INCIDENT PERPETRATED IN THE UNITED STATES BY A MEMBER OF AN INTERNATIONAL TERRORIST ORGANIZATION. DURING 1987, THE FBI RECORDED JUST SEVEN TERRORIST INCIDENTS, ALL OF WHICH OCCURRED ON ONE DAY IN PUERTO RICO. THUS FAR IN 1988, THERE HAVE BEEN TWO TERRORIST INCIDENTS IN THE UNITED STATES OR ITS TERRITORIES, AND THEY ALSO TOOK PLACE IN PUERTO RICO ON THE SAME DAY. WE IN THE FBI BELIEVE THAT THERE ARE SOUND REASONS FOR THE LOW INCIDENCE OF TERRORISM IN THE UNITED STATES.

DURING THE 1960'S AND 1970'S, THE PEOPLE OF OUR NATION WERE SUBJECTED TO A SUBSTANTIAL NUMBER OF TERRORIST INCIDENTS INCLUDING A LARGE NUMBER OF BOMBINGS OF LAW ENFORCEMENT AND

CORPORATE FACILITIES. AMERICAN GOVERNMENT AND BUSINESS ESTABLISHMENTS WERE REGULARLY SINGLED OUT AS TARGETS. AS THE NUMBER OF TERRORIST INCIDENTS GREW IN OUR NATION, WE ALSO SAW A SHARP INCREASE IN ATTACKS ON AMERICANS AND AMERICAN INTERESTS ABROAD BY INTERNATIONAL TERRORISTS. THESE ATTACKS TOOK PLACE IN MANY PARTS OF THE GLOBE. ALTHOUGH NOT DIRECTED AGAINST THE UNITED STATES, MEMBERS OF THE BLACK SEPTEMBER ORGANIZATION, A PALESTINIAN TERRORIST GROUP, DEMONSTRATED AT THE 1972 SUMMER OLYMPIC GAMES IN MUNICH, WEST GERMANY, THAT THEY HAD BOTH THE PROPENSITY AND CAPABILITY TO CONDUCT TERRORIST ACTIVITIES OUTSIDE THE MIDDLE EAST.

IN THE 1970S, THE DOCUMENTATION FOR RECORDING TERRORIST INCIDENTS IN THE UNITED STATES WAS NOT SUBJECT TO THE SAME SCRUTINY THE FBI USES TODAY. WE ESTIMATE THAT TERRORIST INCIDENTS IN THIS COUNTRY AND PUERTO RICO EXCEEDED 100 PER YEAR IN THE MID-1970'S AND, IN FACT, WE RECORDED 112 INCIDENTS IN 1977. THESE INCLUDED INCIDENTS PERPETRATED BY BOTH DOMESTIC AND INTERNATIONAL TERRORIST ORGANIZATIONS.

IN 1982, IN RESPONSE TO THIS WIDELY RECOGNIZED AND GROWING PROBLEM, THE FBI DIRECTOR DESIGNATED THE TERRORISM PROGRAM A NATIONAL PRIORITY. AS SUCH, IT WAS ELEVATED TO A STATUS ON PAR WITH WHITE COLLAR CRIME, ORGANIZED CRIME AND FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS.

THE COUNTERTERRORISM PROGRAM HAS BEEN EXTREMELY SUCCESSFUL. BETWEEN 1980 AND 1982 THERE WERE 122 TERRORIST INCIDENTS IN THE UNITED STATES WITH 51 OCCURRING IN 1982. FROM THAT POINT, THE

NUMBERS HAVE GENERALLY DECLINED TO 31 IN 1983, 12 IN 1984, AND SEVEN IN 1985. DURING 1986 WE RECORDED 24 INCIDENTS, 16 OF WHICH WERE BOMBINGS OR ATTEMPTED BOMBINGS IN PUERTO RICO. AS I HAVE PREVIOUSLY STATED, SEVEN SUCH INCIDENTS WERE RECORDED IN PUERTO RICO IN 1987; TWO TERRORIST INCIDENTS HAVE OCCURRED THERE IN 1988; AND WE HAVE NOT HAD THE COMMISSION OF A TERRORIST INCIDENT IN THIS COUNTRY BY A MEMBER OF AN INTERNATIONAL TERRORIST ORGANIZATION SINCE 1983 DESPITE THE HIGHLY PUBLICIZED EVENTS THESE GROUPS HAVE ORCHESTRATED ABROAD.

THROUGH THE CAREFULLY CONTROLLED COLLECTION OF INTELLIGENCE, COOPERATION, AND DILIGENT INVESTIGATION, THE FBI AND OTHER LAW ENFORCEMENT AGENCIES HAVE BEEN ABLE TO PREVENT AT LEAST 54 TERRORIST INCIDENTS SINCE 1982. IF NOT DETECTED, THESE INCIDENTS WOULD HAVE RESULTED IN A SUBSTANTIAL NUMBER OF CASUALTIES. LET ME HIGHLIGHT SEVERAL EXAMPLES TO ILLUSTRATE MY POINT.

DURING 1983 THE FBI DEVELOPED INFORMATION THAT SEVERAL PRO-KHOMEINI IRANIAN STUDENTS WERE INVOLVED IN A PLAN TO FIREBOMB A SEATTLE, WASHINGTON THEATER WHILE AN IRANIAN THEATRICAL GROUP PERFORMED. THIS PLAN, WHICH COULD HAVE RESULTED IN THE DEATHS OF SEVERAL HUNDRED THEATERGOERS, WAS INTERDICTED WHEN THESE WOULD-BE TERRORISTS WERE SURVEILLED AND THEN INTERVIEWED BY THE FBI AND LOCAL LAW ENFORCEMENT AUTHORITIES PRIOR TO THE PROPOSED FIREBOMBING. THE STUDENTS HAD PLANNED TO ATTACK THE THEATER BECAUSE A LARGE NUMBER OF PRO-SHAH IRANIANS WERE EXPECTED TO ATTEND THIS PERFORMANCE.

DURING JANUARY, 1985, EIGHT INDIVIDUALS WERE ARRESTED BY THE FBI IN MIAMI, FLORIDA IN CONNECTION WITH A PLAN TO STAGE A COUP AGAINST THE GOVERNMENT OF HONDURAS. THE PLAN WAS TO INCLUDE THE ASSASSINATION OF THE INCUMBENT PRESIDENT OF HONDURAS, ROBERTO SUAZO. EIGHT CONVICTIONS AS WELL AS THE SEIZURE OF NARCOTICS RESULTED FROM THIS INVESTIGATION.

IN MAY 1985, BASED ON INFORMATION DEVELOPED BY THE FBI, FIVE SIKH TERRORISTS WERE ARRESTED IN NEW ORLEANS, LOUISIANA ON A VARIETY OF CHARGES. OUR INVESTIGATION DETERMINED THAT THEY HAD PLANNED TWO ASSASSINATIONS: THE CHIEF MINISTER OF THE INDIAN STATE OF HARYANA DURING HIS VISIT TO NEW ORLEANS, AND PRIME MINISTER RAJIV GANDHI DURING HIS VISIT TO THE UNITED STATES IN JUNE, 1985. FOUR OF THE FIVE HAVE BEEN CONVICTED TO DATE.

IN MAY 1986, THE ROYAL CANADIAN MOUNTED POLICE (RCMP) ARRESTED FIVE SIKH TERRORISTS WHO CONSPIRED TO PLACE A BOMB ABOARD AN AIR INDIA AIRLINER AT JOHN F. KENNEDY AIRPORT IN NEW YORK. INFORMATION DEVELOPED JOINTLY BY THE RCMP AND THE FBI LED TO THESE ARRESTS AND ABORTED WHAT COULD HAVE BEEN A DEVASTATING TERRORIST INCIDENT. TWO OF THE FIVE HAVE BEEN SUCCESSFULLY PROSECUTED AND CONVICTED. AS YOU MAY KNOW, SIKH TERRORISTS ARE SUSPECTED IN THE JUNE, 1985, AIR INDIA DISASTER OFF THE COAST OF IRELAND, WHICH CLAIMED 329 LIVES, AND AN EXPLOSION THE SAME DAY IN THE BAGGAGE AREA AT TOKYO'S NARITA AIRPORT KILLING TWO BAGGAGE HANDLERS. SUCH INCIDENTS DEMONSTRATE THAT THESE TERRORISTS ARE WILLING AND CAPABLE OF CARRYING OUT EXTREMELY VIOLENT CRIMINAL ACTIVITY.

DURING JULY 1986, THE FBI, IN CONCERT WITH THE U.S. CUSTOMS SERVICE, DEVELOPED INFORMATION THAT 14 INDIVIDUALS HAD ATTEMPTED TO RECRUIT PERSONS FROM THE UNITED STATES TO TRAVEL TO SURINAME FOR THE PURPOSE OF OVERTHROWING THAT COUNTRY'S GOVERNMENT. AS A RESULT, THEY WERE ARRESTED AND CHARGED WITH VIOLATIONS OF THE NEUTRALITY AND ARMS EXPORT ACTS. ALL 14 PERSONS WERE EVENTUALLY CONVICTED IN THIS CASE.

THERE HAVE BEEN A NUMBER OF INSTANCES IN WHICH INTERNATIONAL TERRORISTS UTILIZED U.S. PERSONS TO CARRY OUT TERRORIST ACTIVITIES IN THE UNITED STATES. AN EXAMPLE IS THE MAY, 1982 ACTION BY INDIVIDUALS BELONGING TO THE ARMENIAN SECRET ARMY FOR THE LIBERATION OF ARMENIA (ASALA) WHO WERE OBSERVED BY THE FBI ATTEMPTING TO BOMB THE AIR CANADA CARGO ENTRY AREA AT LOS ANGELES INTERNATIONAL AIRPORT. AS A RESULT OF THE FBI'S INVESTIGATION, ALL THREE INDIVIDUALS WERE SUBSEQUENTLY ARRESTED AND CONVICTED.

DURING 1985, INDIVIDUALS BELONGING TO THE EL RUKN GANG, AN ORGANIZED CRIMINAL GROUP PRONE TO VIOLENCE, WITH LINKS TO THE LIBYAN GOVERNMENT, WERE ARRESTED BY THE FBI FOR FIREARMS VIOLATIONS. THE ARRESTS WERE MADE AS THEY ATTEMPTED TO PURCHASE A ROCKET THAT WAS TO HAVE BEEN USED IN A TERRORIST ATTACK INVOLVING THE SHOOTING DOWN OF AN AIRLINER TAKING OFF FROM CHICAGO'S O'HARE INTERNATIONAL AIRPORT. FIVE INDIVIDUALS BELONGING TO THIS GROUP HAVE BEEN CONVICTED OF A NUMBER OF CRIMINAL VIOLATIONS IN CONNECTION WITH THIS AND OTHER INCIDENTS.

BOTH OF THE LAST TWO EXAMPLES CLEARLY INDICATE THE POTENTIAL FOR INTERNATIONAL TERRORIST ORGANIZATIONS TO USE U.S. INDIVIDUALS IN EFFORTS TO ENGAGE IN TERRORIST ACTIVITY IN THE UNITED STATES.

THE DOCUMENTED SUCCESS IN PREVENTING TERRORISM IN THE UNITED STATES IS DUE PRIMARILY TO A STRONG FBI COUNTERTERRORISM PROGRAM.

I BELIEVE THAT THERE ARE FIVE OPTIONS THAT CAN BE USED TO FIGHT TERRORISM: DIPLOMACY, ECONOMIC SANCTIONS, COVERT OPERATIONS, MILITARY INTERVENTION, AND LAW ENFORCEMENT ACTION. THE LATTER CAN BE THE MOST EFFECTIVE.

SINCE THE PRIMARY GOAL OF THE FBI IS TO PREVENT A TERRORIST INCIDENT FROM OCCURRING, IT IS ABSOLUTELY ESSENTIAL THAT WE HAVE AN AGGRESSIVE INTELLIGENCE COLLECTION PROGRAM. WE CONTINUE TO FOSTER LIAISON WITH APPROPRIATE FOREIGN LAW ENFORCEMENT AND INTELLIGENCE AGENCIES THROUGH OUR LEGAL ATTACHE PROGRAM. DOMESTICALLY, WE COOPERATE EXTENSIVELY WITH FEDERAL, STATE AND LOCAL AUTHORITIES. UNDER APPROPRIATE CONTROL AND SUPERVISION, INFORMANTS OR INTELLIGENCE ASSETS ARE DEVELOPED AND OPERATED. THE COOPERATION OF ALERT AND CONCERNED CITIZENS IS OFTEN USEFUL.

INFORMATION OF AN INTELLIGENCE NATURE MUST BE CAREFULLY EVALUATED TO DETERMINE ITS VALIDITY. THE FBI DEVOTES CONSIDERABLE EFFORT AND RESOURCES TO THE ANALYSIS OF INFORMATION ACQUIRED. SUCH INFORMATION IS USUALLY INCOMPLETE AND MUST BE PURSUED TO DETERMINE ITS VALIDITY. IT IS THROUGH THIS PROCESS OF ANALYSIS AND INVESTIGATION THAT INTELLIGENCE INFORMATION IS

VETTED AND PRIORITIZED, SOMETIMES LEADING TO THE HARD EVIDENCE NECESSARY TO SEEK PROSECUTION.

NOT ALL INTELLIGENCE LEADS TO PROSECUTIONS. NEVERTHELESS, COUNTERTERRORISM INTELLIGENCE CAN AND SOMETIMES DOES PROVIDE ENOUGH OF A BASIS FOR THE FBI TO PREVENT TERRORIST ACTS FROM OCCURRING.

COOPERATION AND THE SHARING OF INFORMATION AMONG THE WORLD'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES HAVE BEEN TWO OF THE KEYS TO SUCCESS, PARTICULARLY AGAINST INTERNATIONAL TERRORISTS. COOPERATION BETWEEN COUNTRIES HAS BEEN FOSTERED THROUGH SUCH GROUPS AS INTERPOL WHICH HAS DEVELOPED A SPECIAL UNIT TO COMPILE INFORMATION ON TERRORIST GROUPS AND COMMUNICATE THIS INFORMATION THROUGH ITS WORLDWIDE NETWORK. ONE OBJECTIVE OF THIS UNIT IS TO CONDUCT SYMPOSIUMS ON TERRORISM TO BETTER FOSTER COOPERATION AMONG LAW ENFORCEMENT AGENCIES IN THE INTERNATIONAL FIGHT AGAINST TERRORISM.

U.S. GOVERNMENT PARTICIPATION IN VARIOUS BILATERIAL AND MULTILATERAL FORA ALSO MAKES IT POSSIBLE TO SHARE INFORMATION ON INTERNATIONAL TERRORISTS. ADDITIONALLY, PROCLAMATIONS SUCH AS THOSE ISSUED BY THE INDUSTRIALIZED NATIONS COMPRISING THE SUMMIT 7 (THE UNITED STATES, CANADA, FRANCE, THE UNITED KINGDOM, WEST GERMANY, ITALY AND JAPAN) SERVE TO IDENTIFY AND HIGHLIGHT AREAS OF COMMON CONCERN. THE UNITED STATES, THROUGH THE ATTORNEY GENERAL, HAS ESTABLISHED AN INFORMAL BUT PRODUCTIVE RELATIONSHIP WITH THE MINISTERS OF JUSTICE AND INTERIOR OF THE EUROPEAN

ECONOMIC COMMUNITY COUNTRIES IN AN ORGANIZATION KNOWN AS THE TREVI GROUP. TREVI MEETS SEMIANNUALLY TO CONSIDER SPECIFIC MEASURES TO COMBAT TERRORISM THROUGH JOINT INITIATIVES AND COOPERATION.

THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP) IS ALSO TAKING A LEADERSHIP ROLE IN THE FIGHT AGAINST TERRORISM. IN 1986, THE PRESIDENT AND BOARD OF DIRECTORS OF THE IACP CONCLUDED THAT INTERNATIONAL TERRORISM WAS OF SUCH CONCERN TO THE WORLDWIDE POLICE COMMUNITY THAT THE IACP SHOULD ESTABLISH A COMMITTEE ON TERRORISM TO EXAMINE THE ISSUE OF COOPERATIVE POLICE ACTIVITIES IN COMBATTING INTERNATIONAL TERRORISM. THE FBI HAS TAKEN THE LEAD ROLE WITH RESPECT TO THE TERRORISM COMMITTEE AND IS IN THE PROCESS OF MAKING RECOMMENDATIONS TO DEAL WITH A NUMBER OF ISSUES, INCLUDING INFORMATION SHARING AND INTELLIGENCE SYSTEMS, LAW ENFORCEMENT OPERATIONAL CAPABILITIES, THREAT ASSESSMENT/RISK ANALYSIS AND CONTINGENCY PLANNING, AND TRAINING/PUBLIC INFORMATION AS THESE RELATE TO THE TERRORISM PROBLEM.

ALL OF THE ABOVE INITIATIVES ARE BEING PURSUED TO OBTAIN THE COOPERATION AND SUPPORT NECESSARY TO PREVENT TERRORIST ACTS FROM TAKING PLACE. IN THE EVENT WE ARE UNABLE TO PREVENT AN INCIDENT FROM OCCURRING, THE FBI HAS COMPREHENSIVE PLANS FOR RESPONDING TO SUCH INCIDENTS BOTH HERE AND ABROAD. AS YOU KNOW, RECENT CONGRESSIONAL ACTION CREATED EXTRATERRITORIAL JURISDICTION IN CERTAIN CIRCUMSTANCES INVOLVING TERRORISM. THESE ARE EMBODIED IN THE COMPREHENSIVE CRIME CONTROL ACT

OF 1984 AND THE DIPLOMATIC SECURITY AND ANTI-TERRORISM ACT OF 1986. BY ASSIGNMENT OF THE ATTORNEY GENERAL, THE FBI IS THE SOLE AGENCY RESPONSIBLE FOR CRIMINAL INVESTIGATION OF VIOLATIONS INVOLVING THESE STATUTES. IN COOPERATION WITH THE HOST FOREIGN GOVERNMENT, THE FBI UTILIZES INVESTIGATIVE METHODS AND FORENSIC EXAMINATIONS THAT ARE APPROPRIATE UNDER U.S. LAWS AND ACCEPTABLE TO THE GOVERNMENT WHERE THE INCIDENT OCCURRED. NO EFFORT IS SPARED TO IDENTIFY AND BRING TO JUSTICE THOSE WHO ARE RESPONSIBLE FOR TERRORIST ACTS AGAINST U.S. PERSONS OR INTERESTS AS DEFINED BY THESE NEW STATUTES.

WITH REGARD TO DOMESTIC TERRORISTS, WE RECOGNIZE THAT THERE IS MORE TO BE DONE TO PREVENT THIS FORM OF TERRORISM IN OUR COUNTRY. WE DEFINE DOMESTIC TERRORIST GROUPS AS THOSE GROUPS WHICH ARE INDIGENOUS TO THE UNITED STATES AND WHOSE ACTIVITIES DO NOT EXTEND BEYOND THE BORDERS OF THE UNITED STATES OR ITS TERRITORIES. THE FBI IS DEVOTING THE RESOURCES NECESSARY TO DEAL WITH THIS PROBLEM AND, WHERE APPROPRIATE, DOES SO IN CONCERT WITH LOCAL AUTHORITIES.

FOR EXAMPLE, WE HAVE ESTABLISHED 12 JOINT TERRORIST TASK FORCES IN MAJOR CITIES. THESE TASK FORCES, WHICH ARE MADE UP OF FEDERAL, STATE AND LOCAL LAW ENFORCEMENT OFFICERS, WERE ESTABLISHED TO DEAL WITH TERRORISM PROBLEMS IN SPECIFIC AREAS AND TO FACILITATE THE EXCHANGE OF INFORMATION AND JOINT INVESTIGATIVE ACTIVITIES. THIS EFFORT HAS BEEN EXTREMELY SUCCESSFUL IN DETERRING CRIMINAL ACTIVITY OF TERRORISTS AS WELL AS SOLVING CRIMINAL ACTS COMMITTED BY TERRORIST GROUPS AFTER THE FACT.

JUST LAST WEEK THE EXCELLENT WORK OF THE NEW YORK JOINT TERRORIST TASK FORCE LED TO THE CONVICTIONS OF MUTULU SHAKUR AND MARILYN BUCK FOR THEIR PARTICIPATION IN THE 1981 ROBBERY OF AN ARMORED CAR AND THE MURDERS OF A BRINKS GUARD AND TWO POLICE OFFICERS. THEY WERE ALSO CONVICTED OF NUMEROUS OTHER CRIMES AND FACE POSSIBLE LIFE SENTENCES.

ON THE SAME DAY AS THESE CONVICTIONS, A FEDERAL GRAND JURY IN WASHINGTON, D.C., INDICTED SEVEN PERSONS FOR THE 1983 BOMBING OF THE U.S. CAPITOL AND SEVERAL OTHER BOMBINGS OF GOVERNMENT BUILDINGS. ONE OF THOSE INDICTED WAS MARILYN BUCK WHO HAD JUST BEEN CONVICTED IN THE NEW YORK CASE. BOTH THE NEW YORK AND WASHINGTON CASES WERE THE RESULT OF COOPERATIVE LAW ENFORCEMENT EFFORTS LEAD BY THE FBI. I WOULD LIKE TO NOTE THAT THESE INDIVIDUALS ARE HIGHLY INTELLIGENT PEOPLE WHO CONSTITUTED A SOPHISTICATED TERRORIST GROUP. THEY AND OTHERS LIKE THEM COULD HAVE REPRESENTED A THREAT TO THE INFRASTRUCTURE OF THE UNITED STATES IF NOT IDENTIFIED, ARRESTED AND PROSECUTED.

FBI PROJECTIONS FOR FUTURE TERRORIST ACTIVITIES IN THIS COUNTRY ARE BASED ON PAST EXPERIENCE, INTELLIGENCE INFORMATION GLEANED THROUGH OUR INVESTIGATIONS, OUR INFORMANTS AND ASSETS, INFORMATION PROVIDED TO US BY OTHER COMPONENTS OF THE UNITED STATES GOVERNMENT AND THE LAW ENFORCEMENT COMMUNITY AND INFORMATION PROVIDED BY FOREIGN GOVERNMENTS.

AN ANALYSIS OF TERRORIST INCIDENTS BETWEEN 1983 AND THE PRESENT REVEALS THAT 71 OF

THE 83 INCIDENTS WERE ACTUAL OR ATTEMPTED BOMBINGS. THERE HAVE ALSO BEEN SEVERAL SHOOTINGS, ARMED ROBBERIES, ASSASSINATIONS, ASSAULTS AND KIDNAPINGS.

FORTUNATELY, TERRORISTS ACTIVE IN THIS COUNTRY HAVE NOT YET BEGUN TO USE ANYTHING WHICH WE COULD REFER TO AS HIGH TECHNOLOGY TERRORIST IMPLEMENTS. THIS IS NOT TO SAY THAT TERRORISTS DO NOT HAVE ACCESS TO ADVANCED COMMUNICATION DEVICES, REMOTE CONTROL INSTRUMENTS FOR DETONATING EXPLOSIVES, UNDETECTABLE FIREARMS OR EXPLOSIVES, ELECTRONIC SURVEILLANCE DEVICES AND OTHER SUCH TECHNOLOGY. IT IS WELL KNOWN THAT A NUMBER OF THESE ITEMS ARE ACCESSIBLE SHOULD TERRORIST GROUPS CHOOSE TO USE THEM. THE MAY 19TH COMMUNIST ORGANIZATION, WHOSE MEMBERS HAVE JUST BEEN CONVICTED IN NEW YORK, USED THIS TYPE OF EQUIPMENT IN CARRYING OUT THEIR TERRORIST ACTIVITIES.

ALTHOUGH THE UNITED STATES HAS NOT EXPERIENCED AN ACT OF TERRORISM INVOLVING NUCLEAR, CHEMICAL, BIOLOGICAL OR OTHER HIGHLY TECHNICAL WEAPONS, THE FBI HAS AGGRESSIVELY PURSUED THE COORDINATION OF INTERAGENCY OPERATIONAL RESPONSES TO PREPARE FOR CRISES SUCH AS THESE. MUCH OF WHAT WE ARE DOING AND THE INITIATIVES WE ARE TAKING CANNOT BE DISCUSSED IN OPEN SESSION.

OF PARTICULAR CONCERN TO THE FBI IS THE THREAT OF NUCLEAR TERRORISM. THE FBI HAS WORKED TO ESTABLISH A COORDINATED EFFORT FOR RESPONDING TO THREATS OF NUCLEAR TERRORISM. MEMORANDA OF UNDERSTANDING ARE IN PLACE WITH THE DEPARTMENT

OF ENERGY, THE NUCLEAR REGULATORY COMMISSION AND THE DEPARTMENT OF DEFENSE.

WE RECENTLY CONCLUDED A MULTI-AGENCY TRAINING EXERCISE THAT DEALT WITH THE POSSIBILITY OF A SOPHISTICATED NUCLEAR TERRORIST ATTACK AND HAVE CONDUCTED SEVERAL SIMILAR EXERCISES IN THE PAST. THESE TRAINING EXERCISES ARE HELD ON A REGULAR BASIS AND INCLUDE AGENCIES OF THE EXECUTIVE BRANCH WHICH WOULD BE INVOLVED IF SUCH A TERRORIST ATTACK IS ATTEMPTED IN THE UNITED STATES.

ONE OF THE MOST AMBITIOUS PROJECTS CURRENTLY UNDERWAY AT THE FBI IS THE ESTABLISHMENT OF A RESPONSE FOR CHEMICAL AND BIOLOGICAL TERRORISM. ACCORDING TO NEIL C. LIVINGSTONE AND JOSEPH D. DOUGLASS OF THE INSTITUTE FOR FOREIGN POLICY ANALYSIS, INCORPORATED; "THE DANGER OF A TERRORIST GROUP MANUFACTURING OR STEALING LETHAL CHEMICAL OR BIOLOGICAL WEAPONS POSES A GREATER THREAT TO THE AMERICAN NATIONAL SECURITY THAN THE PROSPECT OF TERRORISTS ACQUIRING AN ATOMIC BOMB. CHEMICAL AND BIOLOGICAL WEAPONS ARE MORE EASILY ACQUIRED, CHEAPER TO PRODUCE, MORE DIFFICULT TO DETECT, AND CAN BE EMPLOYED AGAINST ALMOST ANY TARGET. CHEMICAL OR BIOLOGICAL AGENTS DISPERSED IN A CROWDED AREA, PARTICULARLY IN AN ENCLOSED AREA, COULD KILL HUNDREDS TO TENS OF THOUSANDS OF PERSONS."

THE SPREAD OF CHEMICAL WEAPONS IN THIRD WORLD COUNTRIES HAS INCREASED THE POSSIBILITY THAT TERRORISTS WILL ACQUIRE THESE WEAPONS AND THE CAPABILITY TO USE THEM. STATE-SPONSORED

TERRORISM INCREASES THE POTENTIAL FOR SUCH AN INCIDENT. THE FBI HAS ACCEPTED THIS VERY REAL POSSIBILITY AND HAS BEEN WORKING TO DEVELOP AN INTERAGENCY RESPONSE. BY DESIGN, THIS RESPONSE PACKAGE WILL INCLUDE A THREAT ASSESSMENT COMPONENT CAPABLE OF EVALUATING THE CREDIBILITY OF ALL THREATS, AND A MULTIAGENCY RESPONSE TEAM UTILIZING THE EXPERTISE OF THE DEPARTMENT OF DEFENSE AND OTHER FEDERAL AGENCIES, IN CONJUNCTION WITH STATE AND LOCAL AGENCIES. ONCE THE VALIDITY OF A THREAT IS ESTABLISHED, THIS HIGHLY TRAINED REPONSE TEAM WOULD BE DEPLOYED TO THE SCENE TO PROMPTLY RESOLVE THE CRISIS. IN THE EVENT A TERRORIST INCIDENT DOES TAKE PLACE, THE FBI WILL RETAIN MANAGEMENT RESPONSIBILITY FOR DEALING WITH THE LAW ENFORCEMENT ASPECTS OF THE CRISIS. PROCEDURES HAVE BEEN DEVELOPED TO TURN OVER THE MANAGEMENT OF THE CONSEQUENCES OF THE INCIDENT TO THE FEDERAL EMERGENCY MANAGEMENT AGENCY WHEN THE AFTEREFFECTS OF THE INCIDENT FALL WITHIN THEIR MANDATE. THIS PROJECT IS CURRENTLY IN THE PLANNING STAGE.

I NOTED THAT ONE OF YOUR CONCERNS IS THE VULNERABILITY OF THE INFRASTRUCTURE OF THE UNITED STATES TO TERRORIST ATTACK. IT IS READILY APPARENT THAT OUR COUNTRY RELIES HEAVILY ON THE CONTINUITY OF INDUSTRY AND ITS ABILITY TO PRODUCE THOSE GOODS AND SERVICES VITAL TO THE GOVERNMENT AND ITS CITIZENS.

KEY INFRASTUCTURE INDUSTRIES COMMON TO ALL MODERN INDUSTRIAL NATIONS ARE GENERALLY CONSIDERED TO INCLUDE TELECOMMUNICATIONS, TRANSPORTATION, ELECTRICAL POWER, GAS AND OIL, BANKING AND FINANCE AND GOVERNMENT OPERATIONS.

CONCEIVABLY THESE INDUSTRIAL AND ECONOMIC LINCHPINS COULD BE TARGETED FOR A TERRORIST ASSAULT. CONSIDERING THE COMPLEXITIES OF OUR SOCIETY AND THE NUMBER OF INFRASTRUCTURE TARGETS, IT IS UNREALISTIC TO ASSUME THAT WE HAVE THE ABILITY OR RESOURCES TO GUARANTEE PROTECTION TO OUR NATION'S INFRASTRUCTURE INDUSTRIES FROM EVERY CONCEIVABLE TERRORIST ATTACK. RATHER, WE MUST RELY ON THE TIMELY COLLECTION OF INTELLIGENCE INFORMATION TO ENABLE US TO PREVENT AN ATTACK FROM TAKING PLACE.

AS THE LEAD AGENCY FOR COUNTERTERRORISM INVESTIGATIONS IN OUR COUNTRY, THE FBI IS DEVELOPING INITIATIVES DESIGNED TO BETTER ADDRESS THE PROBLEMS RELATED TO A POTENTIAL TERRORIST ATTACK AGAINST ANY ELEMENT OF THE INFRASTRUCTURE. CONSULTATIONS HAVE BEEN UNDERTAKEN WITH OFFICIALS INVOLVED IN KEY INDUSTRIES. WE HAVE ALSO SPOKEN WITH VARIOUS PERSONS IN THE ACADEMIC COMMUNITY WHO HAVE STUDIED INFRASTRUCTURE VULNERABILTY. WE HAVE MADE THIS A HIGH PRIORITY, AND IT IS OUR INTENTION TO WORK WITH OTHER FEDERAL AGENCIES, THE PRIVATE SECTOR AND LOCAL LAW ENFORCEMENT TO ENSURE THE SECURITY OF OUR KEY INFRASTRUCTURE INDUSTRIES.

AMONG THE INITIATIVES TAKEN BY THE FBI IS THE DEVELOPMENT OF A DOMESTIC TERRORIST THREAT WARNING SYSTEM WHEREBY A COORDINATED THREAT WARNING OR ALERT MESSAGE CAN BE TRANSMITTED TO LAW ENFORCEMENT, FEDERAL AGENCIES OR THE TARGETS OF A TERRORIST ATTACK IN A TIMELY MANNER TO DETER OR PREVENT THE TERRORIST FROM CARRYING OUT HIS/HER CRIME.

WE IN THE FBI FIRMLY BELIEVE THAT KNOWLEDGE IS A VALUABLE TOOL IN THE FIGHT AGAINST TERRORISM. OUTSTANDING POLICE WORK SUCH AS THAT EXHIBITED BY TROOPER ROBERT CIEPLENSKY OF THE NEW JERSEY STATE POLICE IN EARLY APRIL WHICH PREEMPTED A POTENTIAL TERRORIST INCIDENT FROM OCCURRING AND THE EXCELLENT WORK DONE BY CHIEF RICHARD JEWETT OF THE RICHFORD, VERMONT POLICE DEPARTMENT LAST FALL POSSIBLY PREVENTED AN INCIDENT OF SOME KIND, WHETHER TERRORIST OR NOT, FROM OCCURRING IN THE UNITED STATES. IN THE NEAR FUTURE, THE FBI WILL SEND BASIC BACKGROUND INFORMATION AND THREAT ASSESSMENTS ON TERRORIST GROUPS AND ORGANIZATIONS TO STATE AND LOCAL LAW ENFORCEMENT AGENCIES SO THEY MIGHT BETTER CARRY OUT THEIR RESPONSIBILITIES. WE RECOGNIZE THAT THE FBI PERSONNEL COMMITTED IN THE COUNTERTERRORISM EFFORT NEED THE HELP AND ASSISTANCE OF ALL LAW ENFORCEMENT OFFICERS IN THE UNITED STATES.

WE KNOW THAT OUR COUNTERTERRORISM PROGRAM IS FAR BETTER TODAY THAN IT WAS IN THE 1970s. IT IS EVEN STRONGER THAN WHEN THE PROGRAM WAS DECLARED A NATIONAL PRIORITY IN 1982. WE ALSO RECOGNIZE THAT THERE ARE MANY THINGS TO BE DONE BUT WE CERTAINLY BELIEVE THAT, AS OUR ACHIEVEMENTS WOULD DEMONSTRATE, WE ARE ON THE RIGHT TRACK. BUT, WE MUST ALWAYS BE PREPARED TO DEAL WITH CHANGES IN THE TACTICS OF TERRORIST GROUPS INCLUDING THEIR ADOPTION OF HIGH TECHNOLOGY EQUIPMENT AND TARGETING OF THE MOST SENSITIVE COMPONENTS OF OUR COMPLEX SOCIETY.

Senator **Leahy**. Ambassador Bremer, I do not mean to cut into your testimony ahead of time, but I think it is a good point to bring you into this on state-sponsored terrorism. How do you see that threat evolving? Is the threat greater in this country from state-sponsored terrorism or from small, radical groups that owe allegiance to nobody but themselves?

STATEMENT OF L. PAUL BREMER

Ambassador **Bremer**. Well, Mr. Chairman, I think an important development in terrorism in the last 10 years has been the emergence of state sponsorship of terrorist groups, particularly Syria, Libya, and Iran.

State sponsorship gives a terrorist group a lot of support such as ready access to finances, some of the things you mentioned, access to diplomatic pouches in embassies, access to transportation, false travel documents, and so forth.

It is a fundamental element of our worldwide counterterrorism policy to try to focus on that state sponsorship, get attention to it, and do something about it. I am reluctant to guess as to whether that is a more dangerous threat within our country than individual terrorist groups.

I think Mr. Revell in his comments has already covered the kind of threat. I think it is true, as I have said in my prepared statement, that it is likely that groups which have access to state sponsorship will more readily be able to move up the escalatory ladder either in high technology or, also conceivably, to mass-casualty terrorism.

Senator **Leahy**. Well, let us go into specifics. Again, if we begin to get into areas that would require going into classified material, just say so and we will understand. We will wait until a later hearing when we can have a classified session, if necessary.

Look at Libya. Every one of us, just reading the papers and without going into any classified material, watches with bated breath what might happen since the bombing in Tripoli a couple of years ago. We did see certain activities 2 years to the day afterward; and then there is the Iran situation, and now we have had a major escalation in the Persian Gulf.

I do not think that anybody here expects that that is going to be the last word in the Gulf. We anticipate that there will be more fighting there. Iran cannot send its navy out to destroy our fleet. Iran, however, could do a great deal of destruction at the World Trade Towers or the Chicago Mart or almost anywhere else in the United States.

What is your judgment of the likelihood of terrorist actions here within the continental United States caused by either Libya or Iran?

Ambassador **Bremer**. I believe that the main reason we have not seen much international terrorism actually conducted in the United States is that it is far easier to conduct attacks against American interests overseas.

If you look at the figures, every year between 20 and 25 percent of all attacks overseas are directed against American interests. In other words, we are a target. In fact, we are the second most likely target of terrorism already.

We have more than 2 million Americans living overseas, almost 300 diplomatic posts, hundreds of military bases, and literally thousands of American companies overseas.

Senator **Leahy**. When you said we are the second most likely, for the sake of everybody who is taking notes, who is first?

Ambassador **Bremer**. Israel.

Senator **Leahy**. OK, go ahead.

Ambassador **Bremer**. In a word, if you are a terrorist state or a terrorist group, there is an abundance of American targets available outside the United States which are, by and large, more readily accessible than coming into the United States. I think that is the primary structural reason why, to date, we have not seen much international terrorism here.

Like Mr. Revell, I agree that good law enforcement and good intelligence has also contributed to keeping that number down. And I agree with him, and your opening comments—I think it would be silly to think that we are going to avoid that forever. We will get international terrorism here at some point, but it is still much easier to attack American targets overseas.

Senator **Leahy**. At some point, somebody is going to start figuring out the psychological effect of bombing our consulate in whatever country, and figure out that while that is very serious and damaging to morale and prestige, it is not the same as a bombing of a major Government function here in Washington, DC, where it is going to be on the news minutes later.

Ambassador **Bremer**. That is true, Mr. Chairman, but the question is, what is the objective of the terrorist group? If the objective is to change our policy, my impression from looking at polls and talking to people—and I would defer to your judgment of your constituents—but my impression is the American people are very solid on a firm policy toward terrorism. In fact, an event like that might be counterproductive for the terrorists' objectives if their objective is to get us to change our policy.

If the objective is purely revenge, that is a different story, but most terrorist groups, despite their apparent irrationality to the rest of us, in fact, operate in a fairly rational frame. They have objectives, they have a purpose for what they are doing.

If they get the American people really excited by terrorism attacks in this country, they have to be uncertain as to what kind of response they get from us. My guess is it would be very vigorous.

Senator **Leahy**. Having said all that—and I take some comfort in what you are saying, not comfort for our installations or citizens abroad—I am sure that you must still coordinate your efforts to make sure that does not happen.

Let us just take a hypothetical situation. Suppose a jumbo jet is hijacked in the United States by foreign terrorists. Are you and Mr. Revell's agency and other appropriate agencies prepared to mobilize and deal with that?

Ambassador **Bremer**. Yes, we are. There is a clear directive that establishes that for international terrorist incidents overseas the Department of State is the lead agency, and we would immediately convene an interagency task force to deal with that.

In the case you have just hypothesized, if it is in the United States, the FBI would be the lead agency and Mr. Revell's organization would set up an operation, coordinating with us. In fact, it has worked that way. We have had examples where it has, in fact, happened.

Senator LEAHY. We have obviously gone beyond the old Dillinger days of somebody pulling up in the big black Buick and jumping out with a Thompson submachine gun, holding up a bank, and hoping to get out of there. We are in the days of very sophisticated systems, communications, weapons, such as we saw in the Kuwaiti Airlines hijacking.

In the press reports and interviews with some of the people on that airline, it appeared that one of the hijackers, at least one of those they may have picked up at some point, was able to fly a 747. I mean, we are getting into a very sophisticated area. Now, they obviously were well aware of how the communications gear worked on that aircraft and everything else about it.

Do you have evidence, Ambassador, that Iran, Libya, and Iraq are giving terrorists greater access to three things—sophisticated devices, training, and tactics?

Ambassador BREMER. I cannot give a full response to that in open session, Mr. Chairman, as you will appreciate. All of those countries have ongoing relationships with various terrorist groups that at various times have included the kinds of things you are talking about.

I might say on the Kuwaiti hijacking, it is an interesting example, particularly for the subject of this hearing. There were sophisticated techniques used by the hijackers, but very low-tech weapons.

Senator LEAHY. Do you want to explain that, please, a little more?

Ambassador BREMER. The weapons that were used were very simple .22 caliber guns and explosives of, so far as we know, no particularly exotic nature. But the techniques that were used, the ability to move around the airplane, the kind of training they had, the fact that someone was at least trained to understand how the plane operated, show that there was a good deal of sophisticated training that went into the operation. But, in fact, very low-tech weapons were used.

So, when we talk about this threat of moving to more sophisticated terrorism, we should not become so transfixed with the exotic ideas of high-tech that we lose track that, in fact, you can use low-tech things in a sophisticated way and still have a fairly devastating incident.

Senator LEAHY. But that goes also to the training. I am concerned about terrorists getting all kinds of specialized knowledge, from psychological training, which is, I think, a pretty significant aspect, to precise details on where everything is located in the target.

If a terrorist tries to get into a building that is protected by all kinds of sophisticated electronic devices, they could be carrying a howitzer and still not get in. I am more worried about the terrorist who has had a lot of electronic training and can get in even though he might be carrying only a .22 pistol. Is that a trend you see happening now?

Ambassador **Bremer**. I think the intelligence community and the rest of us in the counterterrorist community still have to do a lot of thinking and learning about the lessons of the Kuwaiti hijacking before we can draw final conclusions. But we are certainly concerned about it and training is clearly one of the main advantages which a state sponsor of terrorism can give to a group.

Senator **Leahy**. We got a little bit off the subject of a sophisticated terrorist incident here in the United States. Let's suppose a major hijacking or a very large bombing occurs here, and I have been told that the bomb that exploded outside the Marine barracks in Beirut was one of the most powerful conventional-type bombs that we could ever expect anywhere, so we know they can do this.

And let's suppose this causes very significant casualties, major disruption of political or communications or economic infrastructure, and so on. Do you have plans to deal with that here in the United States?

Mr. **Revell**. We do, Senator. We have put together within the United States a number of contingency planning groups. The FBI's responsibility is, first, to prevent the incident, and then to respond to the investigation or the solution of the incident, but also to give information on the crisis to those agencies who are responsible for the treatment, the return of services, the restoration of order, and so forth.

So, we have assumed under the lead agency aspects the lead in planning for the consequences of terrorism. Obviously, organizations such as FEMA and the State and local agencies who have the civil defense type of responsibilities are part and parcel of that.

Also, the various industry associations, the power and electrical associations, the gas and oil and other industries that have a responsibility to provide to the public those resources necessary to keep society functioning, are brought into this planning process. The health care agencies, those who would deal with either biological or chemical aspects, are part of this process.

Now, this is not to the level that we believe we are prepared to deal with any consequence. Frankly, one of the things that we are considering now is a study of the critical infrastructure of the United States and the consequences of an attack on that infrastructure, and Dr. Kupperman will talk about that.

We know that we need to do more. Like any law enforcement agency, we deal pretty much with today's crisis and take care of tomorrow tomorrow. We are trying to get out in front of that and be prepared.

Senator **Leahy**. I understand. I am not suggesting the FBI should be building the hospitals or stockpiling the standby generators or anything else, but your analysis is going to carry a great deal of weight with corporate America—and a number of these things we are talking about are public utilities, gas and electrical utilities—both in terms of how they develop their own safeguards and their security, and also how they may develop redundancies and backup systems.

Ambassador Bremer, when I was reading your testimony over last night, you had made mention in it of a ban on undetectable plastic guns. I happen to agree with what you said. The ban is an anti-terrorism move by Congress, and I hope the administration supports it.

Are some of those types of guns already available abroad?

Ambassador BREMER. There is one gun that has substantial nonmetallic content manufactured in Austria. It is detectable by current metal detection techniques, however.

Senator LEAHY. It is detectable. Are we working with other countries to see if they can start trying to ban some of these?

Ambassador BREMER. Yes; we are having confidential discussions with a number of countries about the problems of the subject of this subcommittee's hearing, high-tech terrorism, and particularly NBC terrorism.

Senator LEAHY. I travel around the world, as you do. I always feel a little bit more comfortable when I have gone in and out of military bases in some countries because the security in some commercial airports is laughable.

I have walked through airports when I had my briefcase full of everything from metal dictating machines to camera equipment and all sorts of things. I have walked through the metal detectors carrying it and not heard a sound.

I remember in one country the detector did beep very loudly and I stopped to wait. Two security people there were deep in conversation and they finally looked at me annoyingly and moved me along; I was holding up the line. I said OK. It made me very nervous until we got to the next airport. I was wondering who had gone on ahead of me and behind me.

Are we trying to make sure we are doing it right here and to bring pressure for more seriousness over there?

Ambassador BREMER. Yes, we are; Congress passed a law several years ago requiring the FAA to conduct periodic inspections of any airport served by American carriers or from which foreign carriers depart to the United States.

I would not want to speak on behalf of the FAA on that except to say that they have a very active program of conducting these inspections. Where they find problems, we have generally had luck correcting them.

I might say, Senator, I think you are right. The airport security in various airports in the world is below standard, but it is also the case that we have made a lot of progress in the last 15 years.

Fifteen years ago, we used to have an international hijacking, on average, every 3 weeks. Two years ago, we had only two hijackings, the lowest number since we started recorded figures. Last year, we had only one. So far this year, we have had one unfortunately bloody hijacking.

But we have, over the years, made it much more difficult. We have not made it impossible. As Mr. Revell suggested in his initial comments, there is no such thing as a 100-percent security, but we keep working at it.

Senator LEAHY. In fact, we no longer have the weekly Atlanta-Havana-Miami run.

Ambassador BREMER. Right.

Senator LEAHY. You said in your statement that the American people would react aggressively to terrorist tactics that brought pictures of dead Americans on the evening news. But if we have real high-tech terrorism, it might not do physical damage—it might be high-tech terrorism that shuts down all the major stock exchanges for a week.

I would assume that that is technically possible?

Ambassador BREMER. I am not technically qualified to answer that question.

Senator LEAHY. Mr. Revell.

Mr. REVELL. Probably more difficult than you might imagine, but certainly it could be disrupted. Whether it could be shut down or not, I think there are alternate means of communication. But, certainly, computer-to-computer links which are so important now in the financial markets, if they were disrupted through either a traumatic event or through a computer virus of some sort, that would have a very devastating effect on the financial community.

Ambassador BREMER. Of course, there might be some Americans who would have been very happy if the stock market had been shut down at various times in the last year.

Senator LEAHY. Some thought that happened last October.

Do you think that would have a profound psychological effect on this country, though?

Ambassador BREMER. Well, Senator, you are the elected politician. I am just a diplomat.

Senator LEAHY. I am just a small-town lawyer, Mr. Ambassador. We can go back and forth and do that bit.

Ambassador BREMER. I think one of the keys to considering this whole area is that the handling of the very first incident, particularly an incident of mass casualties, must be done very well.

It must not succeed because it is the absolute view of everybody in the intelligence community, and those of us who work on terrorism, that if the first incident, whether it is chemical, biological, or mass casualty of some kind, succeeds, we will see copycat terrorism right afterwards. So, it is vitally important that we handle the first incident with firmness.

Mr. REVELL. Senator, I might point out that we do not have a terrorist analogy. We probably do have analogy in the adulteration of medicine and foods, the so-called Tylenol matter, and the very, very vigorous enforcement action that followed that first incident and the number of arrests and convictions, and so forth.

We have now seen that particular phenomenon almost die out, so I think that is analogous to—it could have had a very traumatic effect on the American public, including the financial devastation of an entire industry, but I think very prompt action on the part of the industry itself in improving its safety and procedures and prompt action on behalf of the law enforcement and health communities very much diminished that particular threat.

Senator LEAHY. I may be restating the obvious, but I want to underscore what you just said, Mr. Revell and Mr. Ambassador. How we deal with that first incident, if it happens, is crucible. That, to a large extent, is the reason for this hearing—just how prepared we are to deal with that first time. I agree that will determine to some extent how many more incidents we have to deal with.

It is how well we deal with hijacking threats now that probably keeps us from having so many hijackings.

Ambassador Bremer, there was an article in the New York Times, and I saw it in other places, too, of breaches reported in U.S. computers. It was just a short while ago.

The report said a computer hacker in West Germany was able to break into U.S. computers and a number of networks that our major defense contractors use. Apparently he went through system after system and acquired information on Star Wars, military programs, nuclear weapons deployments, and the like. He has become the envy of my 17-year-old, who is trying to figure out just how to do that.

Now, a couple of days ago I read that someone succeeded in injecting a virus into computer networks in Israel, mainly in the university community. There is great concern that this computer virus would spread throughout the interlocking Israeli computer system and start destroying data or disrupting operations.

Now, is there any evidence at all of terrorist consideration of disrupting computer networks in our country in this way or penetrating computer networks to gain vital information? Do we have any reason to believe that state-sponsored terrorists are interested in computers, either to aid themselves or to hurt us?

Ambassador BREMER. Well, I will let Mr. Revell answer the first part of the question. I think we have seen no convincing intelligence to indicate they are to date, but I will let Mr. Revell answer that.

Senator LEAHY. I am sorry. Would you repeat that?

Ambassador BREMER. There is no convincing intelligence to indicate that they are interested.

Mr. REVELL. We have seen none of the domestic or international groups operating in the United States pay attention toward computer networks or the communications systems associated with computers. That does not mean it is not a potential.

As situations such as the case you spoke of in West Germany with the young German student—obviously, publicity increases the potential for other groups to use these types of tactics.

Senator LEAHY. You do not take any comfort from the fact that it has not happened yet?

Mr. REVELL. No; I might point out, though, that the West German did not get access to classified information, irrespective of what has been reported. He did get into bulletin boards which were an index to classified systems, but he did not get within the classified systems.

Senator LEAHY. But can we be really confident of that? Are you confident that he did not get into anything classified?

Mr. REVELL. I am confident he did not get into them. I think it would be very difficult to get into them. We spend an awful lot of time and money on encrypting our systems and sealing them against intrusion. Nothing is impossible.

Obviously, a state-sponsored terrorist group would have a higher degree of technological capability. I would presume that it could be done, but the time and effort would be substantial, and that is one of the reasons that we have these safeguards built into our classified systems.

Senator LEAHY. Wasn't it at Christmas time that somebody sent a message throughout all the IBM system that showed up on most people's screens? Are you aware of that or have you heard about that?

Mr. Revell. I am not aware of it. Mr. Bayse, who is our technical expert, assistant director in charge of our technical services division, tells me——

Senator Leahy. He is the one my 17-year-old wants to meet. [Laughter.]

Mr. Revell. He tells me that their belief is that that was an insider joke. It was somebody placing that within the system to send a message within the company itself.

Senator Leahy. I will bet it caused great mirth in the board room of IBM. They are noted for that raucous sense of humor there. [Laughter.]

Mr. Revell. I doubt if it brought much levity to the group.

Senator Leahy. Probably just about as much as it would on the top floor of your building.

Mr. Revell. I think you are right.

Senator Leahy. You know, I should note that I sort of picked around Ambassador Bremer's statement earlier without even giving him a chance to make it, and I apologize for that.

Obviously, your statement will be part of the record.

[The statement of Ambassador Bremer follows:]

TESTIMONY OF
L. PAUL BREMER, III
AMBASSADOR-AT-LARGE FOR COUNTER-TERRORISM
ON
HIGH TECHNOLOGY TERRORISM

Mr. Chairman, it is a pleasure to appear before your Committee to discuss the Administration's assessment of the threat presented by high technology terrorism and to brief you on the Administration's response to that threat. Throughout my testimony, I will use the Committee's definition of high technology terrorism: "the actual or potential use of advanced or sophisticated technology by terrorists to achieve their objectives."

With your permission, Mr. Chairman, I propose to address the first two questions you posed to the Administration, the use of sophisticated technologies to conduct the kind of terrorist attacks we have already seen and the possibility of terrorists turning to weapons of mass destruction -- nuclear, biological or chemical weapons. Mr. Oliver Revell of the Federal Bureau of Investigation will direct his remarks to the third question, the vulnerability of America's infrastructure networks to terrorist attack.

To Date, Most Terrorists Use Older Technologies

Our age is almost defined by technological advance. The transistors that were the marvel of the fifties are passe. Much of this testimony was written on a home lap top computer which would have filled an entire room twenty years ago.

Yet terrorists mostly use weapons technologies developed fifty to one hundred years ago -- pistols, hand grenades and machine guns. State Department figures show that the bomb remains the terrorists' preferred weapon. Consistently over the past 20 years, fifty to sixty percent of all terrorist incidents have been bombings, most of which have used explosives and detonators available for decades.

Terrorists generally use the simplest technology available for their attacks. There are solid reasons for them to do so. Simpler technology is less expensive and often more reliable. Low tech equipment is easier to obtain and attracts less attention. A bomb made from agricultural chemicals may not be as powerful as one made from the latest plastic explosives, but anyone can buy and transport a truckload of fertilizer without arousing suspicion. More important, the operatives who carry out the attacks need less training with low tech equipment. Finally, the older weapons and technologies are as effective now as they have been in the past. Terrorists continue to receive wide-ranging publicity for their attacks using older or simpler technology and weaponry.

As the targets originally preferred by terrorists have become "harder," that is to say better defended, terrorists have usually switched targets rather than turn to new technologies to penetrate defenses. When an Embassy is too well protected, terrorists may switch to unprotected individuals or businesses associated with the target country. Or they may decide to attack the same country's Embassy in another nation.

The phenomenon of target switching has been particularly notable in attacks against civil aviation. As enhanced security on flights to Israel made it difficult to smuggle weapons into the cabin, the Japanese Red Army and the Popular Front for the Liberation of Palestine switched targets. Rather than try to seize an aircraft, they checked their grenades and machine guns and attacked passengers in the baggage claim area of Israel's international airport. After examination of checked baggage became more common on high risk flights, targets were switched again and the check-in counters were attacked, for example by the Abu Nidal group at the Rome and Vienna airports in December of 1985. More recently, in Karachi, terrorists chose not to confront security measures in the terminal at all and instead stormed a Pan American airplane from the tarmac.

In short, there is no persuasive evidence yet that the availability of higher technologies has led to their automatic or widespread use by terrorists. In fact, in each of the incidents mentioned above, the terrorist weapons of choice remained largely the same - handguns, automatic weapons, and hand grenades.

New Technologies are Available

There are, however, no grounds for complacency about the utilization of modern technologies. Several terrorist groups have used sophisticated batteries and integrated circuits to improve the timing devices used on bombs. The Provisional Irish Republican Army bomb intended to kill Prime Minister Margaret Thatcher at Brighton Beach three years ago used a long delay timing device (days rather than hours). Terrorists have also used more sophisticated trigger mechanisms for bombs, using radio signals instead of wires leading from the device to a switch. The Greek terrorist group, November 17, used this technique to attack a US military bus last year.

In some cases, the bombs themselves have changed. The Czech plastic explosive Semtex, more powerful and less detectable than traditional explosives, is becoming very popular with those groups which can gain access to it. Lebanese terrorist Mohammed Ali Hammadei, accused of helping direct the hijacking of TWA 847 in 1985, was captured last year trying to enter the Federal Republic of Germany with the volatile liquid explosive methyl nitrate concealed in liquor bottles.

The Popular Front for the Liberation of Palestine-General Command (PFLP-GC) used a modern, but not especially sophisticated technology, when it launched an attack into Israel on motorized hang-gliders. One group in the Far East has used frequency jamming equipment to block police communications during its attacks, while another has constructed and utilized home-made mortars to conduct standoff attacks against buildings and other targets of interest.

There are other off-the-shelf modern technologies or products which have been or could be used by terrorists. Non-metallic weapons made from polymers can cause problems for current detection devices. The terrorists know that certain kinds of explosives are much less susceptible to dogs and mechanical sniffers than others. Night vision devices and stand-off weapons such as mortars and rocket propelled grenades could enhance terrorist capabilities and thus present greater risks. Lasers and high powered microwave transmitters are also potential threats. Increasingly sophisticated and available photo-reproduction equipment can make document forgery easier than in the past.

The Dynamics of Terrorist Weapons and Tactics

While we have some ability to track past uses of modern technologies, we cannot forecast with precision future uses. One thing we can do is watch the dynamic relationship between protective measures and terrorist targeting and tactics. Most of the terrorists' primary targets are better defended today. Secondary and tertiary targets are also being "hardened". So far, when terrorists are presented with a well defended target, they would rather switch than fight. But there may come a point at which our success in protecting current targets will drive terrorists to use new technologies.

Turning to new technologies does, however, present the terrorists some problems. Many of the newer technologies available require greater expertise than members of many terrorist groups now have. Some weapons, such as remotely piloted vehicles and rockets, require considerable space for testing and training. There are entire areas of the world where that much space is simply not available for use as a terrorist firing range. The costs of some new technologies would also be prohibitive for all but the largest and best-financed terrorist organizations.

The requirements for training, money and test areas suggest that the terrorists most likely to employ the products of new technologies are those who already have, or who can acquire, state sponsorship. A sovereign state can dispense sums of money impossible for an organization to raise alone. And almost any country can provide training and testing facilities at a closed military base.

The need for technical expertise could most readily be overcome by terrorist groups whose programmatic objectives already attract to them highly educated individuals. For example, violence-prone elements in some anti-nuclear, extreme environmentalist and animal rights groups might find among their members the expertise requisite to move to "high-tech" terrorism.

Nuclear, Biological and Chemical Terrorism

Much has been said and written in recent years about the possibility of terrorists employing nuclear, chemical or biological terrorism. Our government has confidential assessments on this topic which I would be pleased to discuss in closed session. For this hearing, I can make some general observations.

First, we should understand that there have not been any actual nuclear terrorist attacks and we do not assess that as a likely possibility in the near future. Chemical substances on the other hand have been used for malevolent purposes by a variety of groups and individuals and must be considered as presenting a somewhat more likely terrorist choice.

While not an act of political terrorism, we can remember the poisoning of medicines which have caused deaths in the United States. Though no case in the United States has been traced to political terrorists, the possibility of terrorists ultimately using this tactic against us or other nations is sobering. There have been similar instances in other countries. Several years ago terrorists poisoned Jaffa oranges, which had a disastrous effect on Israeli citrus exports. More recently, a threat to poison the air in another Mediterranean nation with Dioxin -- which was later proven specious -- initially caused grave concern.

According to our analysis, up to now there have been technical and psycho-political constraints on the use of nuclear, biological and chemical (NBC) terrorism.

Technical constraints are especially important when considering nuclear terrorism. While the basic principles of nuclear weaponry are available in any research library, the actual acquisition of the correct materials and assembly of a workable nuclear device remains an immensely complicated undertaking. Moreover, handling nuclear materials can be extremely dangerous to the terrorists. In our view, few groups, and certainly none without considerable state support, have the technical capacity to acquire, fabricate and employ a nuclear device.

Stealing an existing nuclear weapon is a theoretical alternative. However, our government has taken extraordinary precautions to protect against this possibility. It is also conceivable that a state could make a nuclear device available to a terrorist group. However, we also judge this as a remote possibility.

Development of biological and chemical weapons presents similar, although less compelling technical constraints. The major problem here is that the raw materials with which to construct at least a crude chemical or biological device are more readily available to the terrorists than are the materials and equipment needed to develop a nuclear weapon.

For example, virulent biological agents can be grown or acquired from a variety of sources. Toxic chemical materials are of course widely available through manufacture or theft in most open societies. Poisonous gases and chemicals are routinely transported through many countries to support essential economic activities. The accident at the Union Carbide plant at Bhopal, India demonstrates how deadly modern chemicals can be. A deliberate terrorist attack against such a plant or possibly against the transportation vehicles conveying such materials anywhere in the world might have disastrous consequences.

Psycho-Political Constraints on Terrorists

Of course technical barriers can eventually be overcome. However, there also may be some psycho-political constraints to terrorists' use of such weapons. The fundamental question is whether terrorists will actually act to cause mass casualties -- a thousand or more in a single incident -- through the use of nuclear, chemical, or biological terrorism.

Many experts point out that terrorist actions may disgust us, but they are not without a certain logic. Many terrorist acts are intended to accomplish specific political goals in both the short and longer terms. For many groups, the long range goal is often attainment of power in a new or existing sovereign state. These experts believe that terrorist groups have not and will not resort to using weapons causing mass casualties because such an attack would do severe damage to their long-term goals. Put another way, a credible threat to kill 100,000 people in a major city may get a terrorist colleague out of prison. But the general revulsion engendered may make establishment of the new political order impossible, especially if mass casualties occur.

While there is a certain logic here, we should also recognize that terrorists with the technical sophistication to use weapons of mass destruction may very well also have the political sophistication to protect their long-range goals while acting in the nearer term. For example, terrorists could overcome the constraints on using such weapons simply by downscaling the initial weapon so that it produces only a low or moderate number of casualties. This would offer a demonstration of the credibility and lethality of their threat to inflict mass casualties later if their demands are not met now.

Moreover, some terrorist groups are already showing little aversion to inflicting large numbers of casualties. Some radical Sikh and Tamil elements, some groups in Lebanon, and Sendero Luminoso in Peru have used conventional weapons in attacks in which hundreds have died. These groups may be less hesitant than others about switching to even more lethal weapons. Of, if world opinion becomes jaded, these or other terrorist groups could move to mass casualty terrorism to attract attention.

Finally, of course, chemical weapons are known to be in the hands of states such as Iran and Iraq which have practiced terrorism. The world community has shown little outrage at the recent use of chemical weapons by both Iran and Iraq in their war. Perhaps a psychological barrier has already been broken for terrorists to use them.

What Are We Doing About the Threat?

The Administration's response to the threat of high technology terrorism is focussed in the Inter-Departmental Group on Terrorism (IG/T), which I chair. This is because the President has designated the State Department as lead agency on international terrorism. This inter-agency group has directed intelligence analysis into the potential threat from high technology terrorism. The IG/T has also worked to coordinate the U.S. Government's policy response, especially concerning research and development efforts to counter NBC threats.

Under IG/T leadership we are pursuing an aggressive R&D program on emerging technologies which could be used by terrorists or by those fighting terrorism. A distinguished panel of scientists has helped the Inter-Departmental Group on Terrorism identify and prioritize over 70 projects for research. These projects are concentrated in areas where there seems to be no private sector initiative on readily available funding from other government agencies. Our program, funded through a State Department account, has so far allocated $17 million to 22 different projects.

Our concept is to use our limited funds as seed money. Once a project has proven viable, we seek to turn responsibility for project follow up to the appropriate government agency. We have concentrated our R&D effort in five main areas. Two of these in particular may be of interest to this Committee. Specifically, we have devoted a great deal of effort to developing means to detect newer varieties of explosives and detonating mechanisms. We are also attempting to discover new methods and equipment to detect chemical and biological agents.

In the past year, we have begun a program to coordinate our research and development efforts on high technology terrorism with research in like-minded countries. To date we have proposed such activity with the United Kingdom, Canada, the Federal Republic of Germany and Japan. This effort is still in its initial phase, but I am hopeful that it will yield high dividends in future years.

We have also established a Nuclear Biological Chemical (NBC) Working Group. This specialized group is examining our government's capacity to respond to NBC threats. While I cannot go into detail in open session, I can assure you that the federal government has substantial capacity to respond to threats of nuclear terrorism. We are working to develop similar capacities to respond to chemical and biological threats. The NBC working group has also developed an active program of exercises to test our response capability. Various exercises have involved the federal government alone, the federal government coordinating with state and local government, and the federal government acting with other countries.

What Remains to be Done?

The relative scarcity of high tech terrorism up until now gives us no basis for complacency. While I have offered some views about relative threat levels, I must emphasize to you that assessments grounded on predicting terrorist behavior cannot be taken as protection. There is too much uncertainty.

It should be clear that to some extent there is a race between terrorist adaptations of new technologies and the development and application of countermeasures. A key factor will be the U.S. Government's ability to conduct research into countermeasures quickly and effectively. I believe it only prudent that we devote more money to these R&D efforts.

There are also ways in which Congress can help without straining the federal budget. We should work together to examine the possibility of requiring that taggants be included in all explosives, weapons, and ammunition manufactured in or imported into the United States. Such a measure would greatly simplify efforts to detect concealed explosives and weapons and improve our ability to investigate terrorist acts which have already occurred. We should also explore the possibility of taggants for detonators.

Congress has before it pending legislation which would help control the importation, production and possession of non-metallic firearms. This is an area of special concern to the airline industry, indeed to the entire counter-terrorism community. I urge quick and favorable Congressional action on this legislation.

Conclusion

I congratulate the Committee for its initiative in convoking these hearings to examine the risks of high technology terrorism. While the counter-terrorism community's assessment is that current risks are modest, the long-term picture is much less clear. One of the ironies we face is that successful protection of more and more targets may drive terrorists to use higher technologies. That is why it is so important that we work together to turn the new technologies to our advantage in fighting terrorism.

Senator **Leahy**. Now, I wonder if you gentlemen would mind if I invite Dr. Kupperman and Mr. Woolsey to come up to the table? Please stay there, Mr. Revell and Mr. Ambassador. We will get more microphones.

Mr. Ambassador, in your statement on page 14, you said you established nuclear-biological-chemical, or NBC, working groups. I am going to be following up with questions later on on that.

Could you just give us a little bit more about what that does?

Ambassador **Bremer**. Well, in open session I think I can only make a few general points. First of all, the purpose of that group is to try to analyze for us the kinds of threats which we may face in NBC terrorism in the years ahead and, second, to examine our capacity to prevent or react to threats or actual use of such terrorism.

Senator **Leahy**. Do you feel that that group is getting the type of support that it needs both financially and within the various departments involved with it?

Ambassador **Bremer**. It seems to be so far. I would like to point out, Senator, as I pointed out in my statement, that we are also putting quite a lot of emphasis in our research and development, particularly into the areas of biological and chemical terrorism.

We have a small research and development budget which my office manages for the executive branch in counterterrorism technologies. One of the main areas of emphasis has been precisely this area, the detection of biological and chemical agents. I think it is money very well spent and I hope we will be able to count on congressional support for that money in the years ahead.

Senator **Leahy**. I think anyone who has had some of the briefings on that would be supportive.

Dr. Kupperman, I first heard this expression "computer virus" from you a couple of years ago, and I may have read more about it prior to that, but I do not recall. Since you have given me some idea of it, I have started seeing it here and there into the lexicon of concerns that we have to face.

Would you tell us a little bit more about that?

Mr. **Kupperman**. Sure; computer viruses are, in effect, lines of code, computer code. They replicate and they are often designed to take out large hunks of an existing program. They are injected, in a way, into a system's software and can take out thousands of lines of code.

Some call them computer worms. The British call them logic bombs. They can destroy massive investments in systems software. They behave as a virus, in a way, because they replicate and in some cases they are timed to die.

Senator **Leahy**. In some cases, timed to die. Do you mean they come in, do their damage, and are gone?

Mr. **Kupperman**. Yes.

Senator **Leahy**. And you do not find them?

Mr. **Kupperman**. That is right. You do not have the same success which you would with the normal biological analog of antibodies.

Senator **Leahy**. And are you aware of the computer virus question that was raised in Israel?

Mr. **Kupperman**. Yes, I am quite aware of it. It was very frightening to a lot of the security authorities because the computer systems that were involved in Israel were linked to more than purely academic networks. They had links to governmental networks as well, and the security implications are really horrendous.

A virus must be distinguished from the computer hacker who somehow finds a password and gets into an unclassified or even a classified system. The hackers are not destroying the system; they are only obtaining access to information—and I am not trying to minimize that——

Senator LEAHY. They are reading it?

Mr. KUPPERMAN. Yes, getting information, even diverting funds—whereas with the computer virus tremendous destruction can occur.

Senator LEAHY. Dr. Kupperman, I am anticipating some of your remarks in your overview. I will turn it back to you and then to Mr. Woolsey for your overview. Then I want to get back to some questions for the four of you.

PANEL CONSISTING OF ROBERT H. KUPPERMAN, SENIOR ASSOCIATE, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND R. JAMES WOOLSEY, SHEA & GARDNER

STATEMENT OF ROBERT H. KUPPERMAN

Mr. KUPPERMAN. Well, I really want to start off by saying that both Mr. Revell and Ambassador Bremer and their organizations have done extraordinary work and a lot has been accomplished over the past 4 or 5 years or so, particularly the increasing emphasis which has been given to every aspect of terrorism.

On the other hand, I think we are in our infancy in our understanding of the physical and crisis ramifications and the policy implications of high-tech terror, whatever its probability of occurrence.

I think one thing that everyone in the business will agree to is that in some respects terrorism has become far more sophisticated. In the case of the Kuwaiti airliner hijacking, it may have used less sophisticated technologies but the hijackers were trained, they operated efficiently, they knew what they were doing. They understood the airplane, they understood the need to move people around, they understood the counter-psychological techniques to avoid the so-called Stockholm Syndrome, et cetera. They made it almost impossible for a rescue team to be effective.

Indeed, I think that what has happened short of the Kuwaiti incident and the recent explosions in Naples and the arrest of the Japanese terrorists in the United States is that the number of splashy incidents, the incidents that make the headlines, has diminished since the attack on Libya in 1986.

But terrorism, I tell you the obvious, is an unpleasant subject, and when times are calm we have every tendency, I think, to forget it. Nevertheless, in the view of many serious students of terrorism and, more generally, low-intensity conflict, of which terrorism probably is a part, the next administration is not going to be immune from truly devastating attacks.

These are going to occur with increased frequency in many parts of the world, and American interests abroad and Americans themselves are going to be a primary target. I think that we have got to get our act together in terms of what may happen here in the United States. The next administration must face these problems; they are just not going to go away.

When the Reagan administration first came into office, it treated terrorism seriously, but it got so involved with Central America that it began to ignore the problem until embassies began to blow up. I am not talking about the FBI now. I am talking about the degree of emphasis that the White House placed upon the subject.

The April 1986 attack in Libya, I think, went a long way toward abating some of our more recent terrorism problems. It was not until 1986 that we took, I believe, a really concerted, steady effort, and I do compliment the Reagan administration for this.

Intelligence and police cooperation, as well as the sharing of technology and tactics among our allies has never been better. Despite the Iran Contra mess, the efforts of State, Defense, the National Security Council, and the FBI have been of immeasurable value.

Yet, we are now only prepared to deal with yesterday's terrorists. The biggest problem we may face is the emergence of a different breed of terrorist, one with far greater technological talents than we have seen to date, one whose motivation is not fully understood by us. We are unprepared, in my view, to deal with such terrorists.

Our tough-line policy of no concessions to terrorists has got to be upheld if we are going to be able to deal at all from a coping point of view, but the policy will be sorely tested. We lost for a while, embarrassingly, when we had the arms-for-hostages trade in response to far lesser problems than we may see in the future.

We need to think in larger terms, including the challenges posed to emergency preparedness and mobilization by truly devastating terrorist attacks. We must also think in non-traditional military terms and deal with terrorism as part of a continuum of unconventional warfare for which there is no adequate definition and, frankly, no doctrine whatsoever.

All that has been done domestically and internationally is good, but I do not think we have gone far enough. I think the consequences of these attacks are so vast, the technology so available to so many groups, that we cannot ignore the problem, even if we tend to believe or wish to believe that their likelihood is low.

The biggest threat we face is our own complacency. In fact, the terrorist can cause us the most damage by being quiet for a while. We will, of course, respond to their silence—I am talking about our political response, not that of the agencies involved—by ignoring the problem.

For more than a decade, two questions have plagued the law enforcement community. Will international terrorism come to the United States? Will terrorists employ technologically sophisticated tactics? These questions have not been answered. Yet, most analysts whom I know feel that it is inevitable, that it is just absolutely certain that international terrorism is going to come here at some point. And the Bureau, I think, has successfully dealt with some actual cases which they would have to discuss in classified session.

The problem with international terrorists coming here is that they are not going to take the risks [and it is not an easy matter for them to do that, even with an established infrastructure such as the Iranians here], unless there is going to be some high pay-off politically or in terms of the technology of the tactics involved, whether they are going to attack infrastructure or engage in mass killing. They are not, however, going to come here just to set off a pipe bomb, if they are going to come at all.

The possibility of large-scale disruptions and the killing of many innocent people is just not avoidable. If international terrorism does come to the United States, we are going to have to begin to think of emergency preparedness measures and we are going to have to win the first time around.

Not only is there a copycat phenomenon to worry about, there is, in effect, the morale of a large nation and the question of whether it can have confidence in its government to be able to resolve these matters.

Thank you.

Senator LEAHY. Thank you very much, Dr. Kupperman. I agree with what you say. I wish it were not so; we all do.

Mr. Woolsey, I want to give you a chance to give an overview and then I do want to go back to Mr. Bremer and give him a chance to add anything he wants to this.

Mr. Woolsey.

Mr. WOOLSEY. Thank you, Mr. Chairman. Let me just say very briefly that I am delighted to see a congressional committee taking interest in this particular subject. I think it is important, perhaps in the future vitally important to a large number of people.

I would echo what Bob Kupperman said about the excellent work that has been done to date, but also stress that the problem in the future may not be one that we can deal with by using traditional methods.

We have a highly interrelated set of networks in this country—oil and gas pipelines, computer networks, water—and one of the troubling things is that they are so interrelated. Home furnaces, gas station pumps, water and sewage plants, for example, all need grid electricity. Water is needed to fight fires and run powerplants.

In 1977, in the New York black-out, we were just a very short period away from most of the emergency vehicles being out of fuel—the police cars, the ambulances, the fire engines—because the fuel pumps run on electricity.

So, there is a high possibility for terrorist operations to create cascading effects in the networks in the United States, some of them power, some of them transportation, some of them electronic.

If Air Florida flight 90 a few years ago, for example, had gone down 3 or 4 seconds sooner, it would have severed the only major north-south railroad bridge on the East Coast, requiring virtually all rail traffic north-south to be routed through Ohio.

The electronic funds transfer networks in New York move between a quarter and a half of our annual gross national product daily, and most of them are not protected in anywhere nearly the same way that the classified networks which Mr. Revell was referring to are protected.

There is a whole set of things that need to be done to improve the redundancy and the resiliency of our transportation, power, and electronic networks. Some of them are relatively straightforward, some of them are quite expensive.

I do not mean to suggest in any sense that they are a replacement for law enforcement, but by taking away some of the easy options for disrupting these networks, as well as easy ways to kill large numbers of people, I think we can help create problems and difficulties for potential high-technology terrorists that would make Mr. Revell's work and Ambassador Bremer's work perhaps somewhat easier than it otherwise would be.

The problem is—just as is often the case in something that has huge, potential social costs but no immediately clear market costs, as in the environment—it is difficult to go to a bank network and say you should do much more to protect your fund transfers because they feel that it costs money and maybe the other banks are not doing it, and perhaps insurance will cover it, and perhaps it will not happen anyway.

So, the need for the Government to take some sort of a major role in encouraging, leading, analyzing, and helping formulate programs to make long-term improvements in this situation is, I think, very great.

As I say, I think on some of these issues, we have seen some beginnings, but much more so in the arenas which Ambassador Bremer and Mr. Revell were talking about.

Thank you.

[The joint statement of Mr. Kupperman and Mr. Woolsey follows:]

Techno-Terrorism

Testimony before the Technology and Law
Subcommittee of the Judiciary Committee
by
Robert H. Kupperman
Center for Strategic and International Studies
and
R. James Woolsey
Sh[illegible]
[illegible]

For more than a decade, among the many unanswered questions about international terrorism, two have plagued the intelligence and law enforcement communities:

- Will terrorism come to the U.S.?
- Will terrorists employ technologically sophisticated tactics?

No one has answered either of these questions convincingly; yet most analysts feel that international terrorism will come to the U.S. and some fear that terrorist attacks will become increasingly sophisticated, disrupting society and possibly killing thousands.

Until recently, America considered itself relatively immune to terrorist attacks at home. The recent arrest of a Japanese terrorist transporting explosives in New Jersey reminds us that true immunity is illusory.

Approximately 25% of all international terrorist attacks have been directed at Americans and their interests abroad. Previously, there was little need for terrorists to mount the many operational hurdles and risk capture by attempting to export terrorism to the U.S. Indeed, they were almost as well off operating in Europe as they might have been were they engaged in terrorism here. Instant satellite communications guaranteed the publicity they sought, and given the porous borders in Europe their escape following each terrorist incident was nearly assured.

Although there have been several assasinations in the U.S. which have been termed acts of terrorism, almost all terrorism here has been perpetrated by domestic groups, such as the Weather Underground and its offshoots, the FALN, the Croatians and the Jewish Defense League.

Fortunately, the FBI and other law enforcement agencies have done their jobs well. As a result most of these groups have all but disappeared. Other than fringe groups and pathological right wing extremists, one must look towards state sponsorship of terrorism by Iran or Libya should we be attacked at home. The infrastructure and the logistical bases for such terrorism are in place. Under what conditions they will be used is ill-understood.

If international terrorism comes to the U.S., it is likely that its practitioners will do more than just set off a "pipe-bomb." We should assume that their anticipated gains would outweigh the considerable risks they would take. Inexorably, we are led to the prospect of more sophisticated acts of terrorism than we have seen to date, including the assasination of senior government and industrial officials, attacks against electrical power and other networks; and the dispersal of chemical, biological and radiological agents in densely populated areas.

We are fortunate in that terrorists and the nations that sponsor them have thus far calculated that highly disruptive attacks could prove catastrophic to themselves. But, the recent hijacking of a Kuwaiti jumbo jet may prove to be a watershed in sophistication. With Iran's help, the hijackers were supplied with a trained flight engineer or pilot and carefully coordinated communications. Such preparations foreshadow real danger: state sponsored terrorists are undergoing a metamorphosis--from technological clods relying on fanaticism to skilled tactitians.

Tomorrow's terrorists represent a far more potent threat than we have seen to date. The open question is what will happen when the ideologically motivated terrorist merges with the technologically sophisticated and extends his targeting beyond aircraft.

There is little hope that we will solve the religous and territorial disputes in the Mid-East. And separatist groups, such as the ETA and the IRA, will persist--in unending wars that are passed on from father to son.

What is truly troubling is that the terrorists of a decade ago were committed but had few resources. State sponsorship, coupled with the diffusion of technology worldwide, offers today's terrorist access to chemists, microbiologists, physicists and engineers. Moreover, the proliferation of advanced weapons through indiscriminate arms sales by many countries, expands the tactics of terrorism and makes the problem of combating it even more difficult.

Countries such as Iran, Libya and Syria would have a difficult time dealing with us militarily. On numerous occassions, Iran has tried. Unfortunately, Iran's successes have been greater than we might have anticipated. Yet, in the end, if Iran persists in its belligerence towards the U.S., it will have to concentrate on what it can do well.

Terrorism, especially those acts which are truly disruptive, can inflict great pain on the U.S. and its allies. Iran and its cohorts have demonstrated their competence in this pursuit.

Coping With High Tech Terrorism

Terrorists can damage populous, highly industrialized countries in a variety of ways, including radiological attacks that deny access to important buildings, massive killing, and the disruption of critical networks--electrical and natural gas utilities, potable water, communications, electronic funds transfers, and military networks.

Attacks, such as large truck bombs employed by terrorists in Lebanon in 1983, have killed hundreds of Americans. Yet, such attacks pale in comparison to the terrorists use of chemical and biological agents which are readily available.

Chemical warfare agents, such as VX or GB, need not be stolen or synthesized in order to obtain lethal nerve agents. It is easy to obtain TEPP or parathion, which are commercially available, potent insecticides that are almost as toxic as their military counterparts.

Cultures of anthrax, which can be readily grown and whose lethality is incredible, can be found in research labs, some hospitals, and in the soil of cattle country. The terrorist armed with chemical or radiological agents can kill hundreds, possibly thousands of people. By contrast, terrorists armed with biological weaponry, can in principle, kill tens to hundreds of thousands. While it is difficult to rationalize such acts, as regional conflicts expand and terrorism abounds, we would be foolish to believe that mass killing could not result. The use of chemical agents in the Iran-Iraq war is a case in point.

While government uses state-of-the-art technologies in detecting and dealing with nuclear materials and weapons, we are by contrast poorly prepared to cope with the chemical or biological incidents. Even if the probability of such a terrorist incident were low, the human cost of one occuring would be too high to ignore. Do remember, that as far back as 1975, Palestinian terrorists were known to have access to nerve agents.

The tactics of tomorrow's terrorist are not limited to killing on a grand scale. The U.S. is a nation of exceedingly vulnerable networks. At critical nodes there is often little security. Key components are not stockpiled and the networks may not prove robust. It is important, therefore, to assess the extent of these vulnerabilities, analyze cost-effectiveness and determine alternative means of protecting crucial elements of the networks. Thus, we should consider stockpiling very large transformers. Certainly, the big EHV transformers should be protected by more than chain link fences. Moreover, natural gas transmission is even more vulnerable than the electrical power network. Just as the very large custom-made transformers, big compressors should be better protected and possibly stockpiled.

Clearly, it is infeasible to protect every high tension line, switch, transformer, and compressor. We need to be in the business of risk analysis and net assessment. For many years, the GAO has noted these same vulnerabilities.

Certainly, the best outcome would be prevention. Failing that, we will be faced with the problems of containment and restoration. While our law enforcement and intelligence communities have done an absolutely first rate job in foiling many terrorist attacks, the risks of a major attack occuring in the U.S. are steadily increasing. Therefore, in addition to intelligence and law enforcement activities, we must understand that federal, state and local governments may have to cope with an extended blackout or the loss of natural gas transmission and other essential services. Just imagine, the New York metropolitan area without electricity for several weeks. Think of even a short term interruption of natural gas transmission and the problem of relighting pilot lights.

An obvious question arises: Is there an adequate emergency preparedness mechanism, including contingency plans and training, to cope with disasters of this nature? Civil defence has been funded, though meagerly, to cope with the effects of thermal nuclear war, but can we cope with the effects of an extended blackout?

In 1984, the two of us co-chaired America's Hidden Vulnerabilities, a panel report of the CSIS Science and Technology Committee. The report dealt with precisely these problems; its recommendations seem as valid today as they were four years ago.

The study group recommended the following:

> "That the leadership of the U.S. Senate and House of Representatives establish a joint committee charged with analyzing and, where possible, quantifying the critical problems of network vulnerabilities; attracting government and appropriate public attention to those problems; and drafting legislation for enabling and implementing appropriate counteractions.
>
> "That the president establish in the White House a small emergency preparedness and response staff to guide and coordinate federal and state emergency activities and to provide liaison with the joint committee.
>
> "That the National Academy of Engineering establish, with three year initial federal funding, an Inter-Industry Emergency Preparedness Council of industry and academic representatives to provide an industry-government interface with the joint committee and the White House emergency staff and to serve as a pilot instrument for private sector cooperation in emergency planning and the setting of standards."

Let there be no mistake. These recommendations are important, but they are only a starting point. In the four years since these paragraphs were written, the threat of sophisticated terrorism has increased substantially. This means that there is an urgent need for even these modest steps, with much more to be done if we are to fend off potential disaster.

Senator **Leahy**. Mr. Woolsey, on the study on vulnerabilities that you did with Dr. Kupperman, you talked about the Air Florida crash. Are there any ways that we can deal with a threat to what must be thousands of similar bridges?

I can think of some vital links on our interstate highway system and on our rail system, that would be just as vulnerable.

STATEMENT OF R. JAMES WOOLSEY

Mr. **Woolsey**. One cannot guard every power line or every bridge, Mr. Chairman. One can, I think, try to encourage gas and oil pipeline companies to so situate and protect their computers and their compressors so that a very few people in Louisiana could not knock out a very high proportion of the gas transmission to the east coast.

One cannot protect each and every computer net with encryption and special security features, but we could probably do a lot better with some of the very large networks than we do.

It is a process of looking at sensitive nodes, transformers for electric power grids, and so on, and seeing that we have some redundancy and perhaps some stockpiling of components that, in some cases, such as these transformers, often take years to produce.

It is sensible, high-leverage steps—to take away some of the easier things that a high-technology terrorist could focus on that—seem to me to be particularly needed. I think you are absolutely correct that one does not want a society in which all of our railway bridges are guarded. That is not what we are like.

Senator **Leahy**. But there are steps that we do take. Mr. Revell mentioned the Tylenol case earlier. After that case, the pharmaceutical industry started putting the tamper-proof tops and containers, and so on, which we all found a little bit annoying at first. But, now, I suspect that if any one of us were buying something off the shelf and found that it did not have that protection, we would just put it right back.

Mr. **Woolsey**. Absolutely.

Senator **Leahy**. I mean, you just become conditioned to certain steps that an industry can take.

Yes, Dr. Kupperman.

Mr. **Kupperman**. I think the point is that there is no way of protecting everything. On the other hand, it is absolutely inexcusable, it is frightening to realize that very few nodes, comparatively, control much of our electrical power system.

In these cases, without getting into detail about them, they are guarded by no more than a chain link fence. That is dumb.

Senator **Leahy**. Without leading the witness, something that I always tried not—well, I did not always try not to do it; I have to be honest about it. But do we not also have the situation that if some of the nodes were knocked out, we would have no quick and easy replacement for them?

Mr. **Kupperman**. Not only do we not have quick and easy replacements, it is something on the order of 2 to 3 years. There are no sensors in many cases. They are not made in the United States in some cases.

I mean, if one goes beyond the terrorism problem to the more generic national security problem of the mobilization base of this country, we are in trouble.

Senator **Leahy**. Mr. Ambassador.

Ambassador **Bremer**. A lot of what I had in my statement has been covered one way or the other, Mr. Chairman, but I think it is important in general to keep this subject in perspective.

We have to find, as we do in many things in terrorism, the medium ground between complacency and hysteria. I think it is important to remember that to date, anyway, when terrorists historically have been confronted with hardened targets, as they are increasingly overseas in the case of our embassies and military installations, they have preferred to go after other targets. In a word they have preferred to switch rather than fight.

I think that there are some constraints on moving to high-tech or NBC. We have talked about them a bit. It is more expensive. Often, the materials or weapons are harder to get. They require training, often specialized training, and often training areas.

For example, if you are going to use a stand-off RPG instead of running a car bomb into an embassy, you probably need a place where you can test-fire RPG's. Nuclear, biological, and chemical substances particularly also present to the terrorists themselves dangers which are not insignificant.

Now, I do not think there are, however, any grounds for complacency. We have seen what one could define as high-tech terrorism. I have given a number of examples in my statement already, and we pointed out that we think the most likely actors are terrorist groups which have state support or terrorist groups whose programmatic objectives attract to them high-tech people, people who are physicists or chemists, people with a high degree of education. These people then can get across that threshold more easily than many other terrorist groups.

In addition to the research and development and the NBC working group I mentioned, I would want to stress we have also instituted a rather vigorous exercise activity which involves both international and domestic agencies to exercise our capability to respond to these kinds of terrorist incidents. I think we are making some progress there. This is to answer your question about our ability for crisis management.

I think we need to continue to support additional research into these areas with funding, and I think Congress can pick up some of the suggestions that I have made—there are undoubtedly others around—on ways you can help us make it harder for terrorists to get their hands on and use these more exotic technologies.

Senator **Leahy**. We also have got to find ways either by demonstration and sharing of intelligence or by setting up models to get private industry to take some of these steps that Dr. Kupperman talks about—the electric nodes and the fact that some key parts are produced outside this country, maybe custom-produced, and it could take 2 to 3 years in some cases to replace them. These are obvious vulnerabilities, as with our discussion of Louisiana and their gas pipelines, and so on.

Do you see it as a legitimate issue for government to start working with private industry or to continue working with private industry, in some cases possibly even requiring security steps to be taken?

Ambassador **Bremer**. Well, it is somewhat outside the scope of my current responsibilities, but, of course, anything we can do as a nation—and I think it should be broadened.

As Mr. Kupperman has suggested, we are really talking in many ways not just about terrorism, but about our national security capabilities. And, of course, as a concerned American, I think we should be doing that.

Senator **Leahy**. Let me lead into it another way, but it does go inside the area that you are most knowledgeable about. I can think of some countries that I have traveled in where there are constant guerrilla and terrorist attacks.

I remember in one country I was at the ambassador's residence having a briefing from some of our intelligence people and dinner, and he looked at his watch and he said, oh, wait a minute, it is almost 11:00; let us break off a bit and go out in the garden so we can listen to the 11:00 bombing.

I thought he was kidding, and we went out into the garden and it gets to be 11:00, 11:01, 11:02, 11:03, and all of a sudden, boom. Lights flicker up and down and off everywhere, and he says, oh, they are off by 3 minutes.

I mean, this literally happened. It is interesting. I hope that they did not do that just to impress me. I would hate to think I would have that effect going anywhere, but there have been thousands of attacks against energy grids around the world during the past 10 or 15 years.

Mr. **Kupperman**. About 8,000.

Senator **Leahy**. What?

Mr. **Kupperman**. I think the number is about 8,000.

Senator **Leahy**. Now, there have actually been a handful of bombings of power transmission lines here in the United States by domestic terrorist groups, is that correct?

Mr. **Kupperman**. Many by the New World Liberation Front alone in——

Senator **Leahy**. How many?

Mr. **Kupperman**. More than 10 by an outfit called the New World Liberation Front in the 1970's.

Senator **Leahy**. OK. So, now, there we have an energy transmission as an obvious target. Now, do we have any indication that international terrorist groups are looking at our energy transmission grids?

Mr. **Kupperman**. Yes.

Ambassador **Bremer**. There certainly are examples of terrorist groups attacking energy supplies, you are right. There has been a concerted effort in El Salvador, in Colombia, in Peru, and also in West Germany and Luxembourg. Most of these are attacks against individually isolated and unguarded pylons. They knock down the pylons.

I have not seen convincing intelligence of planning by international groups to do that kind of thing here in the United States.

Senator **Leahy**. Dr. Kupperman, do you agree with that?

Mr. KUPPERMAN. The Department of Energy recently issued a warning to the electric power industry that there may be Iranian attacks on electrical power in the United States.

Mr. REVELL. One of the problems we have is sometimes people react when they do not have a good reason to. In my statement, I talk about us setting up a threat warning system. The State Department and the CIA have one for international posts. We are doing one for domestic.

That particular information was not based on solid intelligence and it shows another side of the problem is that if you go out indiscriminantly with too many warnings, then sooner or later those warnings are going to lose their impact.

So, one of the things we are dealing with, domestically, is how to collate, analyze, and disseminate information that has been properly vetted, properly scrutinized, and can be reacted to on an appropriate basis.

Senator LEAHY. Thinking of other briefings I have had in other forums, I am concerned that we may be getting awfully close to some areas that we cannot go into here. I have a number of other questions, but I may submit those in a classified version and we can probably discuss it in another forum.

Mr. KUPPERMAN. Let me mention, if I may——

Senator LEAHY. Yes, Dr. Kupperman.

Mr. KUPPERMAN [continuing]. One incident that is going on now. It is not a terrorist incident at all. It is the failure, the burning up of a communications switch in the Chicago area, and it shut down O'Hare Airport and is preventing telephone communications over a fairly widespread area, and that is just one small switch.

Senator LEAHY. Well, you know, what worries me about that is that in Mr. Revell's prepared statement it said that members of the May 19 Communist Organization that were convicted of terrorism in New York recently used high-technology items in carrying out their activities.

What specifically do you mean by——

Mr. REVELL. Well, the May 19 Communist Organization was the one that attacked this facility, the computer center at the Navy Yard, the Officer's Club at Fort McNair. They had plans to attack the Executive Office Building of the White House, the computer facility in Annapolis, a CIA location.

They were using conventional methods, but they were using highly sophisticated intelligence collection, planning, and the time devices to inflict precise damage at very sensitive locations.

So, while they were not using sophisticated technology to carry out their activities, they were very sophisticated in the use of conventional technologies against targets of some degree of sophistication. Most of these were college-educated. One was an M.D., others had degrees in the physical sciences.

These were people who had the wherewithal to carry out both sophisticated and, if they desired to do so, high-technology attacks, and their target was the U.S. Government and its policies.

Senator LEAHY. If they had been successful in even half of that, we are not really prepared to deal with the damages, let us say, of a major attack on the Executive Office Building.

Mr. REVELL. We are prepared to deal with them. I do not think we are prepared as a nation to deal with some of the horrendous effects that Dr. Kupperman and Mr. Woolsey have indicated are possible, and I would not argue that point.

I do think that we are prepared to deal with the types of attacks that we have experienced in the past or any reasonable escalation of those type of attacks. Obviously, when we had two federal prisons go up—not a terrorism situation, but the Cuban detainees—simultaneously, virtually, it required us to mobilize a substantial portion of our tactical resources.

About two-thirds of the tactical resources of the FBI were deployed to resolve those two incidents. Well, if you multiply that by a number of terrorist incidents around the United States carried out simultaneously, even if they do not use high technology, very quickly our resources could be overrun and we would have to turn to perhaps less well-trained, well-prepared augmentation forces.

That, we are cognizant of, but as Ambassador Bremer indicated, you have to deal with realities and you have to have a balance. So, what we try to do is analyze information, trends, intelligence, and be prepared to deal with that which we most expect.

Senator LEAHY. Well, to anticipate reality, is there any evidence that terrorists have ever attempted to seize either a nuclear device, biological agents, or chemical weapons?

Mr. REVELL. Well, we have eight nuclear extortions. We have had a couple of attacks upon commercial nuclear facilities.

Senator LEAHY. What do you mean by nuclear extortion?

Mr. REVELL. Letters and threats saying that there was a device and if you did not do certain things—they were hoax threats.

We had a facility in Arkansas where they had a 55-gallon drum of arsenic which was to be used in adulterating drinking facilities. We had a group in Philadelphia in the late 1960's, early 1970's, called RAM, the Revolutionary Action Movement, which planned to poison the Philadelphia water supply. They did not realize that they could not do it, but that was their intent. They also planned to create a number of fires and bombings, and then when the police and emergency services came to the scene and when the Red Cross and Salvation Army trucks came up to provide coffee and food, to poison the coffee and food.

So, we have had domestically a number of situations which obviously, if successful, could have resulted in rather catastrophic consequences.

Senator LEAHY. Did anybody else want to answer on that basic question?

Mr. KUPPERMAN. Let me add just a few thoughts. There have been a number of incidents. There was the alphabet bomber in Los Angeles in the 1970's who was an organic chemist who was trying to make Tibun, which is a nerve agent. That same nerve agent was on sale in Berlin in 1975 to Palestinian terrorists. Fortunately, they were caught.

There have been a number of instances involving chemical agents. In Israel not very long ago, canisters of highly toxic chemical agents were found, which distressed them to no end.

I think the real point is that small groups, if they are really intent upon doing things, causing real trouble, just through having an exterminator's license can obtain nerve agents that are 20 to 30 percent as toxic as military nerve agents.

Senator **Leahy**. Well, let me follow on that. We talk about terrorists being somehow in a lab and they have spent all this money and hired the best minds and they are there building a nuclear weapon or a chemical weapon or something like that.

Could you or I just walk into the open market and buy the ingredients to make a chemical weapon of enormous lethality?

Mr. **Kupperman**. If I tell you, yes.

Senator **Leahy**. What?

Mr. **Kupperman**. If I tell you what to get, yes. [Laughter.]

Senator **Leahy**. Well, without giving a cookbook here, give me an idea of what somebody might do.

Mr. **Kupperman**. Well, you can buy pesticides that are extraordinarily potent as far as human lethality is concerned. In the case of military nerve agents, milligram quantities on your skin will kill you.

If you want chemicals that are maybe 20 to 30 percent as toxic, you can buy them commercially as insecticides. For normal use, it has to be diluted. It has adequate warnings. The safety problems of handling it are, nevertheless, not insubstantial.

Biological agents you are not going to get in any substantial quantity, but anyone with access to a university facility laboratory can do some continuous culturing and can grow anthrax. The mean lethal dose of that is 20,000 spores, which weighs approximately a hundred-millionth of a gram.

Senator, we have had one group growing that in Chicago in, again, the early 1970's. Syrian and other governments have actual dispersal weapons of this nature.

Senator **Leahy**. Have actually——

Mr. **Kupperman**. Have dispersal weapons; that is, weapons capable of dispersing these agents. The potential for the dispersal of chemical agents and biological agents, maybe as a poor man's deterrent to nuclear weapons—I do not know—is around, certainly, at the national level.

Unfortunately, there seems to be an eerie coincidence between the nations that have them and the very same nations that support terrorist groups.

Senator **Leahy**. I was looking at the table in your book on the terrorist arsenal where it has the rating of agents in terms of effectiveness. In grams, you have fuel air explosions, 320 million grams; fragmentation cluster bombs, 32 million grams; hydrocyanic acid, 32 million grams; mustard gas, 3,200,000; nerve gas, 800,000; crude nuclear weapons, fissionable material only, 5,000; and then down to anthrax spores, 8.

Mr. **Kupperman**. Yes, that is to have a 50-percent chance of killing everybody in a 1-square-mile area assuming a 5-mile-per-hour wind for chemicals and biologicals.

Senator **Leahy**. I mention that because we can always get the thrillers to fill up a Saturday night talking about somebody trundling down with the nuclear weapon hidden in the U-Haul trailer. Here, we are talking about somebody carrying something much smaller and perhaps easier to get.

Mr. Kupperman. Yes; It is difficult to disperse. I do not want to leave you with the wrong impression about it. While difficult, it can still be dispersed quite efficiently. But, you know, good intelligence, which is maybe the single most important thing that can be done and what I think the Bureau does magnificently, is really what is needed to avoid such attacks.

There is very little that one can do as far as I can tell—and I am very familiar with the techniques of detecting biologicals—to have any really high probability of detecting these agents. You have got to get back to the intent, the understanding of the organizations that would be interested in doing it and their will and their capacity to do it, and any immediate information that you end up with about what they are planning to do.

On the other hand, some things can be done well and there are prophylactic answers to at least some of the network vulnerability questions, because you really can harden certain transformers, you really can make sure that key nodes are protected.

It is expensive, but we have a strategic and critical materials stockpile which is geared for World War II and it is worth maybe $10 to $15 billion. I do not know what it is at this point. Let us sell off some of the nickel ingots, and whatever, and buy some extra transformers, for example.

Senator Leahy. My last question, and I will ask it of each of you, starting with Mr. Woolsey, is this. We are just a few months away from having a new administration and a new Congress. If you wanted to lay down some advice right now for the next Congress or the next administration, what specific thing or things would you recommend that we do to prepare for the threat of high-tech terrorism?

Mr. Woolsey. Well, Mr. Chairman, in this study that Bob Kupperman and I chaired 4 years ago at the Center for Strategic and International Studies, we suggested, really, that three things be done to get started. I think there has been some attention paid to this issue, as Bob said, in the Vice President's review of these matters.

But I do think that it would be important to institutionalize the concern for this type of network vulnerability in high-technology terrorism on the preventive side. I am not speaking now to the intelligence and the side of things that Ambassador Bremer and Mr. Revell deal with, but rather to the institutional changes that might be necessary in what we do.

You do need, I think, a small group in the White House or National Security Council staff to review this. You do need perhaps a joint committee in Congress or, if not that, some ad hoc committee which systemically would go through the infrastructure vulnerabilities in the United States, probably in a classified manner, to help encourage the executive branch and to lead to their correction.

We proposed 4 years ago that the National Academy of Engineering establish a preparedness council with industry to review steps which industry and the Government could take together on a number of these vulnerabilities.

I think that pushing those first-level institutional changes in Congress and executive branch, working together with industry, is a very important first step. In many of these areas we do not really know yet what it would be reasonable to spend money on, what the smart technical solution might be, and we just need to find out.

Senator **LEAHY**. Thank you.

Ambassador Bremer.

Ambassador **BREMER**. It seems to me, Mr. Chairman, that the problem the next administration faces in this area is the same as it faces in all of its policies toward terrorism, and there are four things we need to do.

First of all, we have got to continue to spend money and resources on intelligence. There is, as several witnesses have said, no substitute for good intelligence in counterterrorism. It is the heart of the matter. If you do not have that, you are really put back into a reactive mode and you are always being driven by events.

Second, it is important to continue a policy of firmness toward terrorists, particularly in this field. The first use of this kind of terrorism must not succeed. As part of that general point, it is important to continue to put pressure on the states which sponsor terrorism because as we have indicated this morning, the groups which have access to state sponsorship may be the first ones to turn to this kind of terrorism.

Third, there is no substitute for American leadership. Most of the terrorism directed against us happens overseas. That means we have got to try to bring together some international cooperation on this.

Fourth, we have to keep the American people educated on the problems of terrorism because, as Dr. Kupperman says, people's attention fades.

There are no grounds for complacency in the area and we have got to keep at the fight.

Senator **LEAHY**. Mr. Revell.

Mr. **REVELL**. I would hope that the incoming administration would review the Vice President's task force and reaffirm its findings and its recommendations, and then be constant in pursuing those objectives, reaffirming the policy and placing emphasis on building the structure that can examine the vulnerabilities within the United States and our vulnerabilities internationally, and address them on a systemic rather than a reaction basis, because I think that what I have seen in this is that we tend to react to external stimuli applied by the terrorists and there is a great deal of hustle and bustle. There are hearings up here, there are meetings at the White House, and everybody is rushing around trying to find a way to fix it when the answers have been there all along that we just need to give them constant attention.

I would hope that there would be this constancy of attention at a lower key, but on a constant basis so that we can continue the progress I think we have made.

Senator **LEAHY**. Dr. Kupperman.

Mr. **KUPPERMAN**. Senator, I think that there is not only the constancy of thought and action that is needed. We really have to view terrorism as part of the spectrum of low-intensity conflict. We really have to view it as part of a new world that we are entering into in terms of conflict.

We are not fighting World War II again. It is not the haydays of NATO. We may even end up with accommodations with the Soviets. They were in the business of sponsoring terrorism for a long time. Right now, they are distancing themselves a great deal. Glasnost is occurring.

Let me put it to you this way. I think you have got to treat this business as a genuine, serious, dangerous national security problem to which we have paid all too little attention, despite the really heroic efforts of the Bureau and the State Department.

Senator **LEAHY**. You are saying just because the sun is shining does not mean it is not a good time to fix the leaks in the roof?

Mr. **KUPPERMAN**. Yes.

Senator **LEAHY**. I do not know where I came up with that cornball example. [Laughter.]

I apologize for that, but I thank the four of you because I do have a very real concern about this and I agree absolutely that good intelligence is an absolute necessity.

I think there are a whole lot of steps we can take to make us less vulnerable, and I think we are all wise enough to know that, as we become less vulnerable in certain areas, then perhaps the target of opportunity shifts to another area.

Last, I think it is essential that we have some idea of what might happen after an attack. Mr. Revell, you have just again referenced that, and you all have in one way or another in your statements or in your writings.

As one who thinks that part of our strength is the 200-year adherence to our Constitution, I cannot think of anything that would put more strain on the Constitution of the United States than a very serious terrorist attack or threat of terrorist attack that might endanger or greatly upset the lives of millions and perhaps tens of millions of Americans.

That, in some ways, is probably a far greater threat than anything else we face in terrorism, the threat that it could actually undermine our constitutional framework of government.

So, I do not envy any of you in trying to sort through how we do that balance of protection in an open society. None of us want to give up that open society, and none of us want to give it up to a handful of terrorists.

So, I thank you all very, very much for being here. We will stand in recess and, Mr. Revell and Ambassador Bremer, I will have some further questions of a classified nature for you.

Thank you, Dr. Kupperman, Mr. Woolsey.

[Whereupon, at 11:23 a.m., the subcommittee was adjourned.]

HIGH-TECH TERRORISM

THURSDAY, SEPTEMBER 15, 1988

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:35 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Today, the Subcommittee on Technology and the Law is holding its second hearing on the potential exploitation of technology by terrorists to attack the United States.

Our first hearing, aimed at defining the scope of the problem, was on May 19 of this year. Mr. Revell of the FBI, who is here today, and Ambassador Bremer from the State Department, represented the executive branch. Dr. Robert Kupperman and Mr. James Woolsey testified as nongovernment experts.

In that first hearing, the subcommittee looked at three ways that terrorists might use technology: First, by using sophisticated devices, such as advanced explosives, remote control, secure communications, and so on, to carry out their attacks. Tragically, we may have seen an example of this kind of terrorism in the assassination of Pakistani President Zia and U.S. Ambassador Raphel.

Second, by using or threatening to use extremely lethal materials, such as nuclear, chemical or biological substances, to force the United States to do something it did not want to do. In responses to my written questions after the May 19 hearing, Mr. Revell provided disturbing examples of attempts in the past.

Third, to attack our society's dependence on high technology, such as power grids, computer networks, and transportation lines, that cause us harm or try to change our national policies. Again, we have seen how even minor accidents can disrupt significant parts of our country or major cities in this regard.

Now, the purpose of the hearing today is to examine in some detail how the executive branch is preparing to deal with these kinds of threats to our national security. Before I introduce the witnesses, though, I want to emphasize that the subcommittee is very sensitive to the importance of avoiding any public discussion of information which might help terrorists understand our vulnerabilities.

So, today, we are going to discuss only in general and in unclassified terms how the executive branch is preparing to deal with high-technology terrorism. If it is necessary to go into some areas in classified session, then we will consider having a closed session in a secure room for that purpose.

In all its preparations, including the illustrative scenarios like the commercial airliner shootdown you see over here, the subcommittee has drawn only on books, articles, and studies in the public domain, as well as the unclassified materials provided by the executive branch.

In our open society, information on all these subjects is easily available to anybody who wants to make even the most modest of efforts. It is the subcommittee's view that ignoring that reality is to increase the risk that we might not be prepared to deal with a terrorist attack.

The subcommittee's purpose in having these hearings is to ensure that the executive branch is thinking through the problem of technology and terrorism, is preparing adequately to deter, defeat, or deal with it if it occurs, and is continuing to strengthen its capabilities.

We want to contribute to greater sensitivity to the problem, and to assist, where appropriate, in ensuring that the necessary resources and authorities are available to responsible executive branch agencies.

Our witnesses today are Mr. Oliver B. Revell, who is the Executive Assistant Director of the FBI; Mr. Edward Badolato, the Deputy Assistant Secretary for Energy Emergencies, Department of Energy; Mr. Craig Alderman, Jr., who is the Deputy Under Secretary of Defense for Policy; and Mr. George Woloshyn, who is the Associate Director for National Preparedness of the Federal Emergency Management Agency.

I have your statements. I might say one thing in this regard, Mr. Revell. We have just very recently received the answers from the FBI on the questions that we submitted last spring and, as a result, we have barely had time to go through those at length. It has created a bit of a problem for us because it took so long to get those answers and, as a result, I may have some followup questions after today's hearing based on the answers received.

Now, I have scenarios that we are going to discuss, which were included in letters to all of you, and have since been blown up on charts so that we can put them up here one at a time. We will use them as a focus for questions after you complete your testimony.

Again, we have committees that go into what happens if we have a nuclear war. We certainly discuss how we avoid nuclear war. Arms control agreements have been signed; others are being negotiated.

But a lot of us have a concern about what appears to be even a greater danger or a more likely possibility than a nuclear war. That is a terrorist attack using technoterrorism.

We are highly vulnerable in an open, highly sophisticated society like ours. Our very sophistication and technological advances create their own kinds of vulnerabilities.

We can see what happens if our communications system, power system, transportation system is disrupted by technoterrorism. We certainly know in our major cities how vulnerable a population is to the kind of biological or chemical warfare that could be used against a concentrated population.

While we welcome super-power nuclear negotiations, unfortunately, the kinds of terrorist attacks we could face would come from people with whom we do not negotiate.

So, Mr. Revell, I would turn to you to give the opening statement. I would ask each person if they could keep their statement relatively short. We will go from Mr. Revell to Mr. Badolato to Mr. Woloshyn and then to Mr. Alderman, and then open it up to questions of the panel at large.

Mr. Revell.

PANEL CONSISTING OF OLIVER B. REVELL, EXECUTIVE ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION; EDWARD V. BADOLATO, DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES, U.S. DEPARTMENT OF ENERGY; GEORGE WOLOSHYN, ASSOCIATE DIRECTOR, NATIONAL PREPAREDNESS DIRECTORATE, FEDERAL EMERGENCY MANAGEMENT AGENCY; AND CRAIG ALDERMAN, JR., DEPUTY UNDER SECRETARY FOR POLICY, DEPARTMENT OF DEFENSE

STATEMENT OF OLIVER B. REVELL

Mr. REVELL. All right, sir. You have a more complete statement, but I would like to highlight maybe three or four paragraphs, if I might.

I am pleased to be back again to discuss this issue, the potential of terrorist exploitation of technology, and, more specifically, how the FBI is developing, along with others, plans to deter, contain, react to, and recover from such attacks.

As I pointed out in my previous testimony before this subcommittee on May 19, during the 1980's the United States has not experienced the high levels of terrorist incidents that have occurred in other nations.

In fact, since 1983, there has not been a successful terrorist incident perpetrated in the United States by a member of an international terrorist organization, although—and I would state this and you have seen the material that we have submitted—although there have been several attempts that could have had disastrous results.

It is through the careful collection and analysis of intelligence information, interagency cooperation, and diligent investigation that the FBI and other law enforcement agencies have been able to prevent at least 54 terrorist incidents since 1982.

The prevention of terrorist incidents in the United States is our primary goal. We have had outstanding success in achieving this goal. However, without the ability to collect intelligence as presently allowed by both the Foreign Intelligence Surveillance Act and the Attorney General's guidelines, we will not be able to protect the American public or the international community in the United States from the violent attacks of international terrorists.

What this is, Mr. Chairman, is a statement that in a free and open society you cannot build a fortress; you cannot protect all of the valuable assets of the country by physical security means.

So, we have placed, and I think we will have to continue to place our primary emphasis on trying to prevent the acts of terrorists by the careful collection and analysis of intelligence for preventive purposes.

However, we obviously must plan for the possible consequences of such an act, and therefore we are engaged in a coordinated interagency process to prepare for such contingencies.

The FBI recognizes our continuing responsibility as the lead Federal agency for terrorism in the United States to prepare ourselves and others to deal with the changes in tactics of terrorist groups.

We have intensified our efforts in a relatively short period of time to address the issues which we will be discussing today. However, we are keenly aware that much work remains to be done before we are able to effectively counter the high-tech terrorist threat.

The subcommittee can rest assured that we, along with the other agencies represented here today, will continue to work diligently to create effective programs to protect this country from the employment of high-technology weapons or targeting of high-technology resources by modern-day terrorists, and as we prepare to meet this challenge our adherence to prescribed investigative guidelines will ensure compliance with constitutionally-protected privileges.

We certainly cannot create a situation where a rush to react to incidents would put us in the position of undertaking activities that in the long term would be detrimental to our society.

Thank you, Mr. Chairman.

[The statement of Mr. Revell follows:]

OPENING STATEMENT OF
OLIVER B. REVELL
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

Mr. Chairman, I am pleased to appear before you to further discuss the issue of potential terrorist exploitation of technology, and more specifically, how the FBI is developing plans to deter, contain, react to, and recover from such attacks. As I pointed out in my previous testimony before this Subcommittee on May 19, 1988, during the 1980s the United States has not experienced the high levels of terrorist incidents that have occurred in other nations of the world. In fact, since 1983, there has not been a successful terrorist incident perpetrated in the United States by a member of an international terrorist organization although there have been several attempts that could have had disastrous results. It is through the careful collection and analysis of intelligence information, interagency cooperation, and diligent investigation that the FBI, and other law enforcement agencies have been able to prevent at least fifty-four terrorist incidents since 1982. The prevention of terrorist incidents in the United States is our primary goal. We have had outstanding success in achieving this goal. However, without the ability to collect intelligence as presently allowed by both the Foreign Intelligence Surveillance Act and the Attorney General Guidelines we will not be able to protect the American public or the international community in the United States from the violent attacks of international terrorists.

In response to additional questions submitted by the Subcommittee subsequent to my last appearance, you have been provided with background information relating to the fifty-four terrorist incidents prevented. As you can see from a review of this data, had these incidents not been detected and interdicted, a substantial number of our citizens and others would have been victims of violent terrorist attacks.

In response to the written questions I have just mentioned, the Subcommittee has been provided with information concerning the FBI's 12 Joint Terrorism Task Forces. These Task Forces were formed because we recognized the concurrent responsibility of the involved agencies. I am convinced that this marshaling of forces has resulted in a more effective use of combined law enforcement resources by eliminating the duplication of investigative efforts. By combining investigative expertise, law enforcement can effectively respond to terrorist threats within the United States. Furthermore, we have found that the cross training of personnel assigned to these task forces has become a potent weapon in our national counterterrorism effort.

This Subcommittee has also been provided with information concerning the FBI's proposed response capability to chemical and biological terrorism. Although these efforts are for the most part classified, the following information can be provided to the Subcommittee: The FBI's response plan will include a threat assessment component capable of evaluating threat credibility and a multiagency response team utilizing the expertise of the Department of Defense and other Federal agencies in conjunction with state and local agencies. Once the validity of a terrorist threat is established, this highly trained response team would be deployed to the scene of a chemical/biological incident to support law enforcement in the resolution of the crisis. Each of the FBI's 58 field offices will have contingency plans formulated specifically to address a chemical or a biological terrorist crisis. Additionally, we intend to provide specialized training to our Special Agents in Charge and other senior management personnel to ensure that the FBI can quickly and effectively deal with such a crisis.

In addition to the above, the FBI has also established a Nuclear Counterterrorism Program. The goal of this program is to both prevent incidents of nuclear terrorism and to respond effectively should an incident occur. In an effort to prevent such terrorist activity, the FBI cooperates with the Department of Energy, the Department of Defense and the Nuclear Regulatory Commission in the exchange of intelligence information and in the assessment of potential threats. In the event of an actual nuclear incident, the FBI has contingency plans with every U.S. nuclear facility. This program is supported by signed Memoranda of Understanding among the FBI and other involved Federal agencies.

Another area addressed in the responses to the Subcommittee's inquiries concerned the development of the FBI's Infrastructure Vulnerability/Key Asset Plan. The FBI's objective in this area is to develop, implement, and maintain a national program which addresses potential and actual acts of terrorism directed against key assets of the infrastructure of the United States. The foundation of this plan rests on the tasking of the FBI's 58 field offices to identify specific key assets, establish liaison with the owners and operators of those assets, and the formulation of contingency plans for those assets aimed at preventing and effectively reacting to a terrorist attack. This program involves cooperative planning with other Government agencies, including the Commander in Chief, United States Forces Command, Federal Emergency Management Agency, Department of Energy; the Committee on Terrorism of the International Association of Chiefs of Police; private industry; and independent research groups.

I am sure that today, as we discuss the scenarios dealing with the shooting down of a commercial airliner; the biological threat to New York City; and the electrical energy threat, that the role of the FBI in preventing and interdicting terrorist incidents which involve the use of high technology will become clearer to the Subcommittee. As I stated in my last appearance before you, we know that our Counterterrorism Program is far better today than it was in the 1970s, and is even stronger than when the program was declared a national priority in 1982.

The FBI recognizes our continuing responsibility as the lead Federal agency for terrorism in the United States to prepare ourselves and others to deal with changes in the tactics of terrorist groups. We have intensified our efforts in a relatively short period of time, to address the issues which we will be discussing today. However, we are keenly aware that much work remains to be done before we are able to effectively counter the high-tech terrorist threat.

The Subcommittee can rest assured that we, along with the other agencies represented here today, will continue to work diligently to create effective programs to protect this country from the employment of high technology weapons or targeting of high technology resources by modern day terrorists. And, as we prepare to meet this challenge, our adherence to prescribed investigative guidelines will ensure compliance with constitutionally protected privileges.

Senator **Leahy**. Thank you very much, Mr. Revell.

As I said before, we will next go to Mr. Badolato from the Department of Energy.

STATEMENT OF EDWARD V. BADOLATO

Mr. **Badolato**. Yes, sir; thank you, Mr. Chairman. I appreciate the opportunity to appear before you today to discuss energy emergency preparedness, with particular emphasis on concerns that terrorists might attack domestic energy systems.

To support the administration's goal of ensuring that consumers have an adequate supply of energy at reasonable cost, the Department of Energy's Energy Emergency Preparedness Program seeks to reduce the Nation's vulnerability to energy supply disruptions and to enhance our ability to respond, should a disruption occur.

We appreciate your understanding of the sensitivity of the details of this subject, and I will orient my remarks to accommodate these sensitivities.

I would like to briefly outline three aspects of the DOE response to the vulnerability of our Nation's energy infrastructure. First, it involves activities undertaken in advance to mitigate the risk of experiencing a major disruption; second, the energy emergency management system in DOE which is to cope with a disruption; and, finally, the nature of response actions which would occur.

The electric power supply disruption postulated in your scenario is severe and unprecedented. Since the 1965 New York City blackout, which was much less severe than your scenario, much has been done and still more actions are underway to mitigate the risks and impacts of severe power supply disruptions.

For example, the electric utility industry formed the North American Electric Reliability Council, or NERC, to ensure adequacy and reliability in utility planning and operations.

Also, DOE has conducted a vigorous program of exercises involving such scenarios as a blackout of electric power in the Northeast and a disruption of all energy forms to the San Francisco area. Similar regional exercises have been conducted with participation by nearly every one of the States.

Also, at the request of DOE, NERC has formed the National Electric Security Committee to develop proposals for industry initiatives to reduce the vulnerability of electric power systems to technoterrorism.

Additionally, as part of the National Security Council's Senior Interagency Group for National Security Emergency Preparedness—that is, SIG on NSEP—the Interagency Group on Energy Vulnerability was established. The purpose of this group is to focus on national policy issues relating to the vulnerability of U.S. energy systems and to develop policy options to mitigate this vulnerability.

We are also working with the energy industry to improve physical security through outreach programs, threat briefings, and so forth. Additionally, our physical security training experts are providing industry training on physical security for their systems.

We have also established a procedure for ensuring that intelligence community threat advisories will be transmitted to the energy industry when appropriate, and we are pleased that the FBI is planning to take responsibility for these activities in the future.

Additionally, the National Communications System has formed an energy task force under DOE encouragement. This task force is meeting with the electric power industry to identify cross-industry needs so that accommodating plans can be developed for use during emergencies.

During a disruption, we would institute our energy emergency management system. DOE would take the lead for the Federal Government in the response and restoration of energy systems.

Overall, the Federal, State, and industry responses would curtail demand, implement service priorities reflecting essential national security and State and local needs, and facilitate reconstitution of the electric power transmission system.

We will work very hard to ensure that this system would meet the needs of the Nation in restoring power, restoring energy, and restoring fuel. All of these actions, Mr. Chairman, are part of an overall energy emergency preparedness program that has been instituted by the Department of Energy.

This concludes my prepared testimony. I will be happy to answer any questions on the scenario at a later time.

[The statement of Mr. Badolato follows:]

STATEMENT OF EDWARD V. BADOLATO
DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES
U.S. DEPARTMENT OF ENERGY

Mr. Chairman and Members of the Subcommittee, I appreciate this opportunity to appear before you today to discuss energy emergency preparedness with particular emphasis on concerns that terrorists might attack domestic energy systems.

To support the Administration's goal of ensuring that consumers have an adequate supply of energy at reasonable cost, the Department of Energy's energy emergency preparedness program seeks to reduce the Nation's vulnerability to energy supply disruptions and to enhance our ability to respond should a disruption occur. As you may imagine, matters dealing with the vulnerabilities of our domestic energy systems become quite sensitive and must be handled delicately lest we create a shopping list for those who would do them harm. Accordingly, we have undertaken a number of important, but low key, initiatives with federal and state agencies and the energy industries with the goal of reducing the vulnerability of our energy supplies. In view of the open style of this hearing, I will restrain my remarks to accommodate these sensitivities.

As requested for discussion purposes, my remarks address an electric power disruption, referred to as Technoterrorism Scenario 3. The Department of Energy (DOE) is not involved with the other two scenarios. I will also refer briefly to DOE's capability to respond to another type of technoterrorism, nuclear terrorism.

In the hypothetical mid-winter electric power disruption scenario, terrorists simultaneously bomb transformers and switches in the northeastern United States. The attacks cause a major disruption of electricity in the northeast. After two weeks, only 35% of electricity in the area has been restored, with New York City receiving less than 50% of its requirements. Related problems include traffic light failures and abandoned vehicles causing massive traffic jams which block emergency vehicles, isolation of a light water nuclear power reactor from the grid, and partial failure of the gas pipeline system because of lack of power.

I would like to briefly discuss three aspects of this scenario: first, activities undertaken in advance to mitigate the risk of experiencing such a disruption; second, the Energy Emergency Management System for coping with a disruption; and, finally, the nature of response actions which would occur. My discussion is intentionally general in nature. Some details, if needed, should be discussed in closed session or be provided in classified form.

The specified electric power supply disruption is severe and unprecedented, with only 35% of electricity supplies to the Northeast having been restored after two weeks. After past bulk power supply system disruptions, service restoration time has been measured in terms of minutes, hours, or a day or so, at most. For example, full restoration took 13 hours in the 1965 New York City blackout. Restoration of the 1977 New York City blackout took 25 hours.

In all past electricity disruptions, electric utilities have restored service without federal assistance. Primary reliance for service restoration continues to be on electric utilities.

However, much has been done and more actions are underway to mitigate the risk of experiencing severe power supply disruptions. For example, following the 1965 New York City blackout, the electric utility industry formed the North American Electric Reliability Council (NERC) to ensure that adequacy and reliability are properly considered in utility planning and operations.

With specific reference to electric power disruptions which might result from technoterrorism:

- DOE has conducted exercises involving such scenarios in the northeast in April 1987 and in the San Francisco area in December 1987. Similar exercises have been conducted during the past five months with participation by emergency personnel from most of the "lower 48" states' energy offices. These exercises permit us to identify potential problems and to test crisis management plans.

- At the request of DOE's Office of Energy Emergencies, NERC formed the National Electric Security Committee to develop proposals to reduce the vulnerability of electric power systems to technoterrorism. The Committee submitted its recommendations in July and the matter is on the agenda of the NERC's October board meeting.

- As part of the National Security Council's Senior Interagency Group for National Security Emergency Preparedness, the Interagency Group on Energy Vulnerability (IG-EV) was established. The purpose of the IG-EV is to focus on national policy issues relating to the vulnerability of U.S. energy systems and develop policy options to mitigate this vulnerability.

  In addition to receiving regular briefings on current energy developments and on events in the energy area that are of particular interest to Federal agencies, the IG-EV publishes a classified twice-yearly report on the world petroleum situation. It is also working on two major projects: (1) energy crisis management plans reflecting national defense priorities, and (2) mitigating the risk of disruption of energy supply systems by technoterrorism.

- DOE is also working with the energy industry to improve physical security through outreach programs. Threat briefings are provided to industry officials. Physical security training is provided by DOE's Central Training Academy.

  Computer programs for assessing physical security vulnerability and suggestions for cost effective improvements will be made available to industry.

- DOE has implemented a procedure for ensuring that intelligence community threat advisories will be transmitted to the energy industry, when appropriate. We are pleased that the FBI is planning to take over this responsibility.

- The industry advisory committee of the National Communications System has formed an Electric Power Task Force. The Task Force is meeting with representatives of the electric power industry for the purpose of identifying what each industry needs from the other during emergencies, and developing cooperative service restoration procedures.

Office of Energy Emergencies

DOE's Office of Energy Emergencies (OEE) has led the Department's efforts to carry out its non-nuclear emergency preparedness strategies. OEE's mission is to assure that adequate U.S. energy is available, at reasonable cost, to support national priorities during emergencies. As shown in Figure 1, three Offices under my leadership carry out this mission.

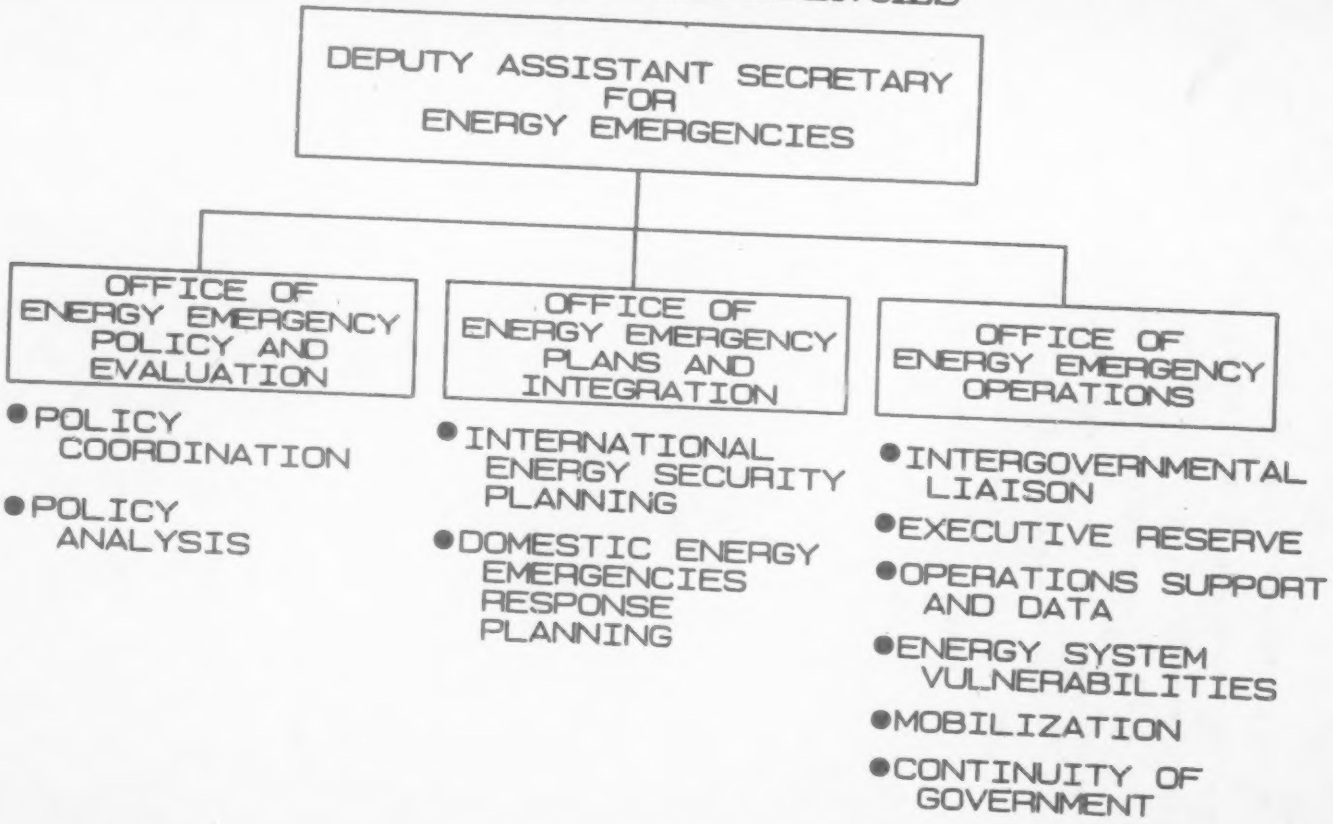
1. The Office of Energy Emergency Policy and Evaluation: Monitors, evaluates, incorporates, and disseminates energy emergency initiatives and developments in support of the OEE preparedness mission.

2. The Office of Energy Emergency Plans and Integration: Develops energy emergency response plans that include the use of the Strategic Petroleum Reserve and the strengthening of commitments to the International Energy Agency and the North Atlantic Treaty Organization.

3. The Office of Energy Emergency Operations: Undertakes efforts to ensure that the U.S. infrastructure (i.e., industry, state and local governments) is able to meet national priorities in the event of catastrophic and defense-related emergencies.

FIGURE 1

OFFICE OF THE DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES


DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES
OFFICE OF ENERGY EMERGENCY POLICY AND EVALUATION
● POLICY COORDINATION
● POLICY ANALYSIS
OFFICE OF ENERGY EMERGENCY PLANS AND INTEGRATION
● INTERNATIONAL ENERGY SECURITY PLANNING
● DOMESTIC ENERGY EMERGENCIES RESPONSE PLANNING
OFFICE OF ENERGY EMERGENCY OPERATIONS
● INTERGOVERNMENTAL LIAISON
● EXECUTIVE RESERVE
● OPERATIONS SUPPORT AND DATA
● ENERGY SYSTEM VULNERABILITIES
● MOBILIZATION
● CONTINUITY OF GOVERNMENT

In the performance of its mission, OEE draws upon the resources and activities of other DOE offices and also coordinates with other government agencies and industry for energy emergency planning and procedures. A broad spectrum of energy emergencies...peacetime through war...involves the resources of OEE. Natural disasters, political disruption, terrorism, and sabotage have highest peacetime priority. Crisis and wartime priorities involve energy emergency preparation for mobilization, conventional and nuclear war.

The way in which DOE responds to energy emergencies involves general and operational planning, procedures, budget and, most important, human resources. An effective crisis management system requires an experienced, mature, well-trained staff that is flexible enough to plan for and respond to a variety of emergency situations. The 71 professional and support staff in the current organization of OEE include experts in oil, natural gas, electric power and coal, as well as economists, engineers, analysts, computer programmers, data processors and administrative staff. To be ready for an unexpected emergency, the staff receives, on a continuing basis, advanced training both in technical and managerial skills. This emphasis on training and preparation has the objective of ensuring that DOE has a relatively small, technically competent staff that is well versed in energy crisis management policy and procedures and is capable of rapidly responding to emergencies.

Many natural and man-made events can cause disruptions of the domestic energy supply system. Some of these, such as equipment failure or an act of vandalism, are routinely handled by industry, while large regional problems, such as the aftermath of an earthquake or potential multisite sabotage, may be serious enough to require government coordination or assistance.

Multisite sabotage and terrorist incidents represent potential threats in the United States. Worldwide, terrorism incidents have been rising about 15 percent a year over the past five years, according to State Department data. In the United States, we have been relatively fortunate because the few acts of sabotage committed against our electric power systems have not reached levels of severity sufficient to cause a major sustained outage. However, some third world countries have experienced substantial power system disruptions (e.g., El Salvador, Peru, Chile, Colombia, Mozambique, Afghanistan and Guatemala).

Terrorist organizations also have attacked power facilities in Western Europe. In the past, these attacks generally were poorly designed and executed, but recent attacks by the same organizations have shown a higher level of technology and better planning. This may portend more effective actions against power systems in the future.

Energy-related terrorism in the United States would be a particularly significant threat in a time of national defense mobilization. The Soviet Union has an unconventional warfare capability (i.e., Spetsnaz units) which has assigned missions to cripple the West's industrial infrastructure, particularly its vulnerable energy systems, prior to an outbreak of hostilities. While the Spetsnaz focus appears to be on Western Europe, the potential for such actions in the United States cannot be dismissed. However, even in the absence of a superpower confrontation, there is the possibility that potential third world adversaries could sponsor attacks on the energy infrastructure in the United States, and OEE is working with industry to mitigate this problem.

From an emergency preparedness standpoint, OEE's first priority effort is on the bulk electric power system which is vital to economic and social stability and to national security. Electric power is uniquely vulnerable because, unlike coal or oil, it cannot be stored and must be available at the instant of demand. Over 142,000 miles of bulk power transmission lines (230kV and above)...many stretching over remote and unprotected areas...connect the Nation's power plants to the distribution companies serving local consumers. Although seldom the cause of a serious disruption to supply, transmission lines have been the most common targets for terrorist groups. Substations, most of which are isolated and unprotected, are particularly exposed.

This problem is exacerbated because many critical components cannot be easily replaced, with repair or replacement times possibly measured in weeks or months.

The petroleum industry enjoys a high priority in U.S. domestic emergency preparedness policy for coping with vulnerability. Its major points of vulnerability are pipelines, refineries, and storage facilities. However, both source and transportation flexibilities tend to reduce the potential impacts of disruptions to petroleum supply. For example, crude oil and petroleum products can be purchased from other sources (e.g., imports) and transported by several modes including water, rail, and fuel trucks.

Natural gas systems are particularly exposed with the most vulnerable components being pipeline interconnections, river crossings, compressor stations, and city gate stations. Dual fuel capability in many industries would mitigate, to some extent, the impacts of a major disruption to the domestic supply of natural gas.

Although coal supplies nearly 25% of our energy, the dispersed nature of the supply system makes it unlikely that even a large hostile action could have a major national impact.

The DOE program of vulnerability reduction and mitigation consists of four phases, as follows:

Phase 1 (DOE/Industry). In-house case studies and simulations to assess the vulnerabilities of candidate energy systems;

Phase 2 (DOE/Industry). Outreach to industry owners and operators to advise of discovered vulnerabilities and to obtain cooperation;

Phase 3 (Industry). Introspective vulnerability assessments by system owners and operators to determine enhancements which may be in accordance with normal business objectives; and

Phase 4 (Interagency Group). Assessments of remaining vulnerabilities and judgments as to whether they constitute an unacceptable risk to national security and, if so, the the kinds of remedies which may be warranted.

The present status of our vulnerability programs is as follows:

ENERGY SYSTEMS	Phase 1 Studies/ Simulations	Phase 2 Cooperation with Industry	Phase 3 Industry Actions	Phase 4 Additional Remedial Initiatives
o Electric Power	Done	Done	In Progress (NERC)	..
o Natural Gas	Done	In Progress	..	..
o Petroleum	Done	In Progress	..	..
o Coal	In Progress	..	..	..

Energy Emergency Management System

DOE utilizes a generalized emergency response process that provides systematic decision-making in response to any energy emergency, whether in electric power, oil, gas, coal, or in the event of an international or domestic energy crisis. The Energy Emergency Management System (EEMS) is organized to assess the nature and extent of an energy emergency and, by drawing upon the total support activities and expertise of DOE, to develop response options. Besides establishing response procedures for each major energy type, the EEMS process also is designed to respond to a variety of possible emergency scenarios, such as an international disruption in oil supplies, defense mobilization, major natural disasters, energy system sabotage, or major accidents involving energy systems.

In the draft DOE Order 5500.5, "Energy Emergency Planning and Management," currently under Departmental review, the EEMS concept is defined and the policies and procedures for administering the EEMS are clearly established, as are the general criteria for developing and coordinating DOE's energy emergency planning activities. As the non-nuclear energy component of DOE's overall Emergency Management System, the order describes the EEMS organizational relationships and integrates its concept of operations into the emergency processes of the Department. The EEMS process has been successfully tested in several large scale exercises.

The key organizational component of EEMS is the Energy Emergency Management Team (EEMT), consisting of a cadre of departmental experts and chaired by me. Figure 2 illustrates the EEMT structure. As DOE's principal internal energy crisis management body, the EEMT has met numerous times in recent months to provide status briefings and projections for the Secretary of Energy on the likely energy impacts of earthquake pipeline damage, events in the Persian Gulf, and electric power supply problems.

In typical situation meetings, the EEMT is provided an up-to-date detailed intelligence briefing, an analysis of the energy impact of the incident, and recommendations for appropriate response actions.

The operational concept of EEMS is illustrated in Figure 3. The continuum begins with routine monitoring of the energy situation to determine whether it is necessary to activate the EEMT and the EEMS process. Next, the situation is analyzed, various response options considered, recommendations made and finally implemented. Each step in the flow of activities allows for termination of the EEMS process if it is no longer necessary, or recycling if the emergency continues.

In the event that the specified Technoterrorism Scenario 3 occurred despite warnings, or in the absence of a warning, the following chain of events would be set in motion:

FIGURE 2

EEMT MEMBERSHIP

CORE GROUP

INTERNATIONAL AFFAIRS AND ENERGY EMERGENCIES

CONGRESSIONAL, INTERGOVERNMENTAL, AND PUBLIC AFFAIRS

GENERAL COUNSEL

DEFENSE PROGRAMS

ENERGY INFORMATION ADMINISTRATION

MANAGEMENT AND ADMINISTRATION

POLICY, PLANNING AND ANALYSIS

OFFICE OF THE UNDER SECRETARY

AUGMENT GROUP

PETROLEUM RESERVES

FOSSIL ENERGY (OTHER THAN PR)

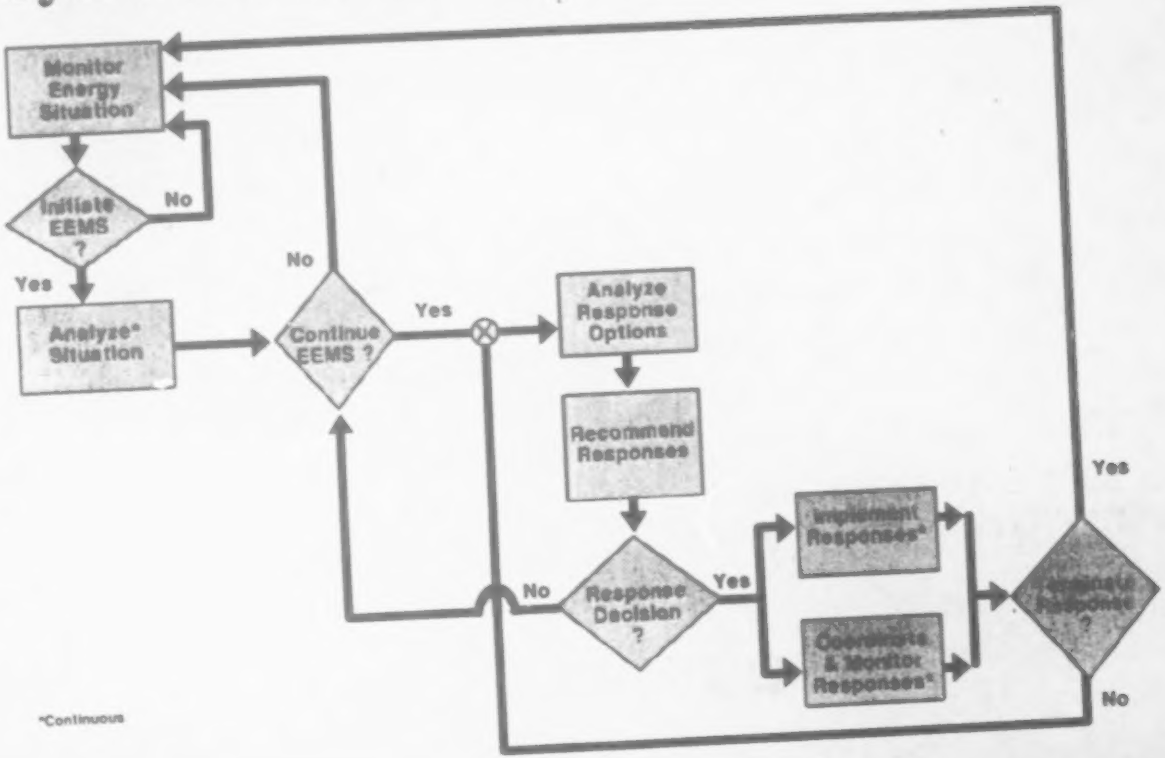
NUCLEAR ENERGY

CONSERVATION AND RENEWABLE ENERGY

ENVIRONMENT, SAFETY, AND HEALTH

FIGURE 3

Energy Emergency Management System: Simplified Diagram


Monitor Energy Situation
Initiate EEMS ?
No
Yes
Analyze* Situation
No
Continue EEMS ?
Yes
Analyze Response Options
Recommend Responses
No
Response Decision ?
Yes
Implement Responses*
Coordinate & Monitor Responses*
Yes
Terminate Response ?
No

*Continuous

Affected utilities would immediately implement local curtailment plans, begin damage assessment and reconstitution planning, and report the incident, as provided by federal regulation, to the DOE Emergency Operations Center.

NERC would notify other utilities throughout the United States and Canada of the incident, using its hotline. Utilities would increase their physical security using in-house resources, available state and local law enforcement personnel, and professional security firms.

The report of an incident of this magnitude would trigger activation of the Energy Emergency Management System. A Situation Analysis would be performed by DOE in cooperation with utilities, state governments, and federal agencies including FEMA, the NRC, and the FBI. The DOE Energy Emergency Management Team would meet to assess the situation, as would the Interagency Group on Energy Vulnerability. The severity of this scenario suggests a war or pre-war situation. If that is the case, a Presidential declaration of a national emergency would likely be recommended. Work on development of federal response options would begin. Under the Executive Branch's lead agency concept, DOE would take the lead for the Federal Government. Overall, the Federal, state, and industry responses developed and implemented would fall into one of three categories. The first category covers responses to limited electricity supplies. Such responses are primarily demand curtailment and implementing service priorities reflecting essential national security and state and local needs. It should be noted that many state emergency plans do not currently consider essential national security needs, a shortcoming that will have to be rectified through a cooperative Federal/state/industry planning effort. The second category consists of reconstruction of the electric power transmission system. Typical response actions to remedy limited electricity supplies and to reconstruct transmission facilities are summarized in Table 1 (attached).

The third category includes responses addressing other problems resulting from the incident, such as physical security of key facilities, and ensuring supplies of fuel for the diesel generators at the nuclear reactor which is isolated from the grid.

If deemed serious enough, the President would declare a national emergency and activate the National Defense Executive Reserves (NDERs). Once activated, the reservists would: (1) advise DOE Headquarters of damage to electric power facilities and availability of power; (2) recommend electric power curtailments as necessary; and (3) recommend restoration priorities, assist in obtaining necessary resources, and monitor restoration work.

TABLE 1

TYPICAL ELECTRICITY RESPONSE OPTIONS

	LEAD		
	Federal	State	Industry
Responses To Limited Electricity Supplies			
Public conservation appeals	X	X	X
Load shifting to off-peak periods			X
Voltage reductions			X
Load shedding		X	X
Identify essential national defense customers to state Public Utility Commissions.	X		
State Public Utility Commissions prioritize service to essential national defense, state and local customers.		X	
Clean Air Act Waiver		X	
NDER Activation (Emergency Electric Power Executive Reserve)	X		
Nuclear plant coastdown or deferred maintenance			X
Accelerate permitting of completed nuclear plants	X		
Increase electricity imports			X
Allocate fuel supplies for electric generation using Defense Production Act (DPA) authorities	X		
Encourage alternate fuel usage where possible	X	X	X
Responses To Reconstitute Electric Supply Systems			
DPA authorities to allocate material, or require priority production of equipment and supplies	X		
DOE coordinates with other federal agencies as needed regarding equipment, skilled labor, transport, communications expediting.	X		
Assistance from non-impacted utilities and equipment manufacturers: replacement components, repair crews, and construction equipment.			X

Public Information activities on the incident would be initiated, including:

- Developing public statements and talking points for key DOE spokesmen;
- Developing background papers and fact sheets explaining DOE response mechanisms;
- Coordinating public information activities with other federal agencies, state and local governments, and the utility industry;
- Responding to media requests for information and interviews;
- Holding or participating in press conferences; and
- Responding to requests from Congress for information, briefings, and hearings.

As necessary and to the extent that they had been identified and appropriately entered into the program, the Defense Department's plans for protecting key energy nodes under their Key Asset Protection Program would be implemented. Under this program, the National Guard and reserves would be used to augment the physical protection of such facilities if necessary.

Nuclear Terrorism

The threat of terrorism directed against the nation's nuclear energy programs has long been a source of major concern in the Department of Energy because of its responsibilities for the protection of nuclear weapons and the research and production facilities which are so important to national security.

Pursuant to Executive Order 11490, as amended, the Department of Energy is assigned responsibility to participate in the conduct, direction, and coordination of search and recovery operations for nuclear material, weapons, or devices; to assist in the identification and deactivation of improvised nuclear devices (INDs) and/or radiological dispersal devices (RDDs); and to render advice on radiation and damage probabilities in the event of the detonation of an IND. This authority complements and is in addition to the Department's general authority under the Atomic

Energy Act of 1954, as amended, and other generic legislation to maintain a technical response capability in a state of readiness to handle nuclear emergencies. The Department also maintains a very close working relationship with the nuclear industry and the Nuclear Regulatory Commission and is fully prepared to assist in the event of a nuclear accident or act of terrorism directed against a commercial nuclear reactor.

There are several actual or potential situations involving nuclear materials which could lead to a DOE response. These include:

- Acts of terrorism
- Extortion
- Stolen material
- Lost or missing material
- Dispersed material
- Material offered for sale illegally.

Countering nuclear threats requires teamwork by federal, state, and local agencies. The FBI has overall jurisdiction at the federal level and is responsible for the legal aspects of any counterthreat actions taken. DOE has the capability of providing technical personnel and equipment to assist in locating, characterizing, and neutralizing nuclear threat devices. To provide appropriate technical assistance promptly, the Nuclear Emergency Search Team (NEST), under the operational control of the Manager, Nevada Operations Office (NV), has been created by DOE to provide the capability to respond to these specialized nuclear emergencies. Many NEST capabilities are also applicable to nonnuclear emergencies and could be made available to assist the FBI on a case-by-case basis, as required.

NEST personnel and equipment are prepared to:

1. Evaluate the credibility of a nuclear threat;
2. Search for a nuclear threat device or radioactive material;
3. Identify the kind and quantity of radioactive materials involved;

4. Assess the probability of nuclear explosive yield or spread of radioactive material;

5. Assess the potential for personnel injury and property damage in the event of activation of a threat device; and

6. Assist in the render safe and disposal operations.

The need for a specialized emergency response team such as NEST is infrequent. Therefore, the majority of NEST personnel are assigned to other tasks in their day-to-day work but remain on-call for a NEST activity as required. The majority of personnel who have volunteered for NEST field assignments are involved in other DOE nuclear programs, especially the nuclear weapons program. Most of these personnel are from DOE's Nevada Operations Office (DOE/NV), Los Alamos National Laboratory, Lawrence Livermore National Laboratory (LLNL), Sandia National Laboratories, and EG&G/EM, Inc. Under an interagency cooperative agreement, Explosive Ordnance Disposal experts from the Department of Defense will participate with DOE/NEST personnel in dealing with a nuclear threat, when warranted by the nature of the problem.

The following outlines the approximate sequence of events in a "classical" NEST scenario:

- FBI informs DOE Headquarters through DOE's Emergency Operations Center (EOC) that a nuclear threat has been received, and provides the threat message together with any other available pertinent information.

- The EOC passes the above information to the Communicated Threat Coordination Center at LLNL which commences the threat assessment process.

- The EOC passes the same information to DOE/NV which relays it to appropriate members of the NEST Community.

- If or when it appears possible that a deployment of NEST personnel and equipment may be directed, each NEST organization is asked to assume an alert posture: locate appropriate personnel and have them stand by on-call; assemble appropriate equipment and prepare it for shipment; and maintain a communications watch so they can be contacted and respond quickly if a deployment is ordered.

This concludes my prepared testimony. I will be happy to answer your questions.

Senator **Leahy**. Thank you very much for that.
Mr. Woloshyn.

STATEMENT OF GEORGE WOLOSHYN

Mr. **Woloshyn**. Mr. Chairman, it is a pleasure to appear before your committee to discuss potential terrorist exploitation of technology and how the administration would deal with these incidents.

We have previously submitted a complete statement for the record, but I would like to summarize a few key points concerning FEMA's role in responding to terrorist incidents.

Under the authority of Executive Order No. 12148, FEMA has been delegated the responsibility for the coordination of preparedness and planning to reduce the consequences of major domestic terrorist incidents.

FEMA is not an intelligence-gathering agency and maintains no intelligence files. We are not a law enforcement agency and do not coordinate any law enforcement plans. Nor are we a regulatory or resource agency with detailed expertise and authorities over critical and potentially vulnerable infrastructure systems, such as energy, transportation, communications, or water resources.

But we do have responsibility in ascertaining that the executive branch can respond in an efficient and coordinated fashion to mitigate the damage, injuries, and disruptions that may result from a severe terrorist incident. In other words, we share responsibility in redressing the consequences of terrorism.

FEMA regards consequences of terrorism as similar to consequences of other types of large-scale catastrophic events or extraordinary situations. The same needs may exist—medical care, food, shelter, evacuation, and so forth, and the same responses and capabilities are called for—coordination, emergency operating centers, emergency communication and data systems, and emergency response capability.

FEMA has made important and visible strides in improving the capability of Federal departments and agencies to respond to major emergencies. We have helped develop plans, communications, information systems, response teams, interagency procedures, and training for all levels of government.

We have assisted the Domestic Policy Council in developing a generic national system for emergency coordination. This plan provides both flexibility and consistency in a coordinated Federal, State, and local effort to assist stricken communities.

If a major terrorist event occurs as stated in your scenarios, the Federal Government will supplement, not supplant, State and local government agencies in responding to its consequences.

Our plans call for the establishment of a Federal response center and joint information center in or near the affected areas, and to support these field operations with existing emergency operating centers and information systems.

To support the Federal response center, FEMA has developed a nationwide emergency communication and information system. This system provides for connectivity with the White House, Department of Defense, Health and Human Services, and other Federal, State, and local components.

FEMA has also been working closely with other agencies in the development and sharing of emergency data bases, an automated modeling capability. This data is used to develop projections, analyses, and options to support decisionmaking.

Not only do we develop plans and supporting communication and information systems, but we also periodically exercise and test Federal, State, and local response capabilities. We sponsor or participate in literally dozens of exercises annually.

These exercises, involving thousands of observers and participants, provide valuable insight into our strengths and weaknesses, and result in remedial actions. A fairly high percentage of these exercises involve technological terrorism, including the use of nuclear and chemical devices.

In short, FEMA plays a valuable role in serving as a focal point for the integration of the various governmental and private sector capabilities into a coherent, coordinated response entity.

The only resources we contribute directly are our professional emergency management skills, our knowledge of various plans and procedures, our understanding of the roles and limitations of the many participants, our mobile and fixed communication and information systems, and our acceptance as a coordinating center for notification, information, and decisionmaking. FEMA also serves as a channel for Presidentially declared Federal disasters.

This concludes my opening statement. I look forward to discussing your three terrorist scenarios involving the use of high technology.

[The prepared statement of Mr. Woloshyn follows:]

STATEMENT OF

THE HONORABLE GEORGE WOLOSHYN

ASSOCIATE DIRECTOR

NATIONAL PREPAREDNESS DIRECTORATE

FEDERAL EMERGENCY MANAGEMENT AGENCY

MR. CHAIRMAN, IT IS A PLEASURE TO APPEAR BEFORE YOUR COMMITTEE TO DISCUSS THE ISSUE OF POTENTIAL TERRORIST EXPLOITATION OF TECHNOLOGY TO ATTACK THIS COUNTRY AND HOW THE ADMINISTRATION WOULD DEAL WITH THESE TYPES OF TERRORIST INCIDENTS.

THE PRINCIPAL FOCUS OF MY TESTIMONY WILL BE ON FEMA'S RESPONSIBILITY IN PREPARING FOR AND RESPONDING TO THE CONSEQUENCES OF MAJOR TERRORIST ATTACKS ON THE UNITED STATES USING SOPHISTICATED TECHNOLOGIES. THE ADMINISTRATION'S RESPONSE TO THE THREAT OF TECHNOLOGICAL TERRORISM IS FOCUSED IN THE INTERDEPARTMENTAL GROUP ON TERRORISM (IG/T), WHICH IS CHAIRED BY L. PAUL BREMER, III, AMBASSADOR-AT-LARGE FOR COUNTER-TERRORISM, DEPARTMENT OF STATE. THREE LEAD AGENCY ASSIGNMENTS ARE IN PLACE FOR MANAGING TERRORIST INCIDENTS THE DEPARTMENT OF STATE FOR INCIDENTS OCCURRING OUTSIDE THE UNITED STATES; THE DEPARTMENT OF JUSTICE (FBI) FOR INCIDENTS WITHIN THE UNITED STATES; AND THE FEDERAL AVIATION ADMINISTRATION FOR THE DEPARTMENT OF TRANSPORTATION FOR HIJACKED AIRCRAFT IN FLIGHT.

UNDER THE AUTHORITY OF EXECUTIVE ORDER 12148, FEMA HAS BEEN DELEGATED THE RESPONSIBILITY FOR THE COORDINATION OF PREPAREDNESS AND PLANNING TO REDUCE THE CONSEQUENCES OF MAJOR TERRORIST INCIDENTS WITHIN THE UNITED STATES. FEMA IS NOT AN INTELLIGENCE GATHERING AGENCY AND MAINTAINS NO INTELLIGENCE FILES. WE DEPEND UPON THOSE AGENCIES WHICH HAVE A LEGAL CHARTER TO COLLECT AND DISSEMINATE INTELLIGENCE. WE ARE NOT A LAW ENFORCEMENT AGENCY AND DO NOT COORDINATE ANY LAW ENFORCEMENT PLANS. FEMA REGARDS CONSEQUENCES OF TERRORISM AS SIMILAR TO CONSEQUENCES OF OTHER TYPES OF LARGE SCALE CATASTROPHIC EVENTS OR EXTRAORDINARY SITUATIONS. THE SAME NEEDS MAY EXIST, E.G. MEDICAL CARE, FOOD, SHELTER, EVACUATION, ETC., AND THE SAME RESPONSES

AND CAPABILITIES ARE CALLED FOR: COORDINATION, EMERGENCY OPERATING CENTERS, AND EMERGENCY RESPONSE CAPABILITY.

FEMA HAS MADE IMPORTANT AND VISIBLE STRIDES IN IMPROVING THE CAPABILITY OF THE FEDERAL DEPARTMENTS AND AGENCIES TO RESPOND TO MAJOR EMERGENCIES OR EXTRAORDINARY SITUATIONS. FEMA HAS HELPED DEVELOP PLANS, COMMUNICATIONS SYSTEMS, RESPONSE TEAMS, INTERAGENCY PROCEDURES, AND TRAINING FOR ALL LEVELS OF GOVERNMENT.

FEMA HAS ASSISTED THE DOMESTIC POLICY COUNCIL IN DEVELOPING THE NATIONAL SYSTEM FOR EMERGENCY COORDINATION (NSEC), WHICH IS A MECHANISM FOR ENSURING THAT THE FEDERAL GOVERNMENT PROVIDES TIMELY, EFFECTIVE, AND COORDINATED ASSISTANCE TO STATES AND LOCAL GOVERNMENTS IN EXTREME CATASTROPHIC TECHNOLOGICAL, NATURAL OR OTHER DOMESTIC DISASTERS OF NATIONAL SIGNIFICANCE. RESPONSIBILITIES CURRENTLY ASSIGNED TO FEDERAL DEPARTMENTS AND AGENCIES BY STATUTE OR OTHER AUTHORITY, AND EXISTING EMERGENCY MANAGEMENT SYSTEMS AND CAPABILITIES, ARE AN INTEGRAL PART OF THIS RESPONSE SYSTEM AND WILL BE USED WHEN POSSIBLE.

ANOTHER EXAMPLE IS THE DEVELOPMENT OF THE FEDERAL RADIOLOGICAL EMERGENCY PLAN (FRERP). FEMA SERVED AS OVERALL COORDINATOR IN DEVELOPING THIS PLAN. THIS JOINT UNDERTAKING OF ALL THE AGENCIES, WHICH WOULD RESPOND TO ANY INCIDENT INVOLVING RADIOACTIVE MATERIALS, INCLUDING NUCLEAR TERRORISM, CULMINATED IN NUMEROUS MAJOR FIELD EXERCISES, SOME INVOLVING APPROXIMATELY 2,000 FEDERAL, STATE, LOCAL AND PRIVATE SECTOR PERSONNEL. THESE EXERCISES HAVE DEMONSTRATED THE EFFECTIVENESS OF A FEDERAL RESPONSE IN SUPPORT OF STATE AND LOCAL GOVERNMENTS AND THE ABILITY OF ALL RESPONDERS TO WORK TOGETHER.

ANOTHER MAJOR STEP WAS THE CAPABILITY FEMA DEVELOPED IN RESPONSE TO WHITE HOUSE TASKING IN COORDINATION WITH OTHER FEDERAL AGENCIES FOR PLANNING AND RESPONDING TO POTENTIAL CATASTROPHIC EMERGENCIES AT THE 1984 SUMMER OLYMPICS. THE PLAN WAS TITLED, "A NATIONAL CONTINGENCY PLAN FOR RESPONDING TO THE CONSEQUENCES OF AN EXTRAORDINARY SITUATION AT SPECIAL EVENTS." THIS NATIONAL CONTINGENCY PLAN OUTLINES HOW FEDERAL DEPARTMENTS AND AGENCIES WOULD RESPOND TO THE CONSEQUENCES OF AN EXTRAORDINARY SITUATION OR AN EMERGENCY THAT COULD THREATEN

THE PUBLIC HEALTH AND SAFETY DURING SPECIAL EVENTS. THIS PLAN WAS ALSO IMPLEMENTED AGAIN DURING THE FOLLOWING SPECIAL EVENTS:

- ° 1984 NEW ORLEANS WORLD'S FAIR
- ° 1984 AND 1988 REPUBLICAN AND DEMOCRATIC NATIONAL CONVENTIONS
- ° 1985 PRESIDENTIAL INAUGURATION
- ° 1987 PAN AMERICAN GAMES

THE MITIGATION OF AND/OR RESPONSE TO THE THREAT OF HIGH TECHNOLOGY TERRORISM AS OUTLINED IN YOUR ILLUSTRATIVE SCENARIOS REQUIRES THE EFFECTIVE PERFORMANCE OF A SET OF INTEGRATED FUNCTIONS BY LOCAL, STATE, AND FEDERAL LEVELS OF GOVERNMENT. AT EACH LEVEL OF GOVERNMENT, MULTIPLE AGENCIES MAY EACH PERFORM SEVERAL DISTINCT PREVENTION/RESPONSE FUNCTIONS. SOME OF THESE FUNCTIONS ARE LARGELY OR ENTIRELY A STATE OR LOCAL PREROGATIVE AND RESPONSIBILITY. OTHER FUNCTIONS ARE THE RESPONSIBILITY OF AND ARE PERFORMED LARGELY BY FEDERAL AGENCIES. YET OTHERS ARE PERFORMED JOINTLY BY STATE AND FEDERAL AGENCIES OR LARGELY, PERHAPS ENTIRELY, BY FEDERAL AGENCIES IN INSTANCES WHERE THERE IS A PRESIDENTIAL DISASTER DECLARATION.

IF A MAJOR TERRORIST EVENT OCCURS AS STATED IN YOUR THREE SCENARIOS, FEMA WILL WORK WITH FEDERAL, STATE, AND LOCAL GOVERNMENT AGENCIES AND THE PRIVATE SECTOR IN RESPONDING TO, AND RECOVERING FROM THE CONSEQUENCES OF ALL TYPES OF EXTRAORDINARY SITUATIONS, INCLUDING TERRORIST INCIDENTS.

OUR PLANS CALL FOR THE ESTABLISHMENT OF A FEDERAL RESPONSE CENTER AND JOINT INFORMATION CENTER IN, OR NEAR, THE AFFECTED AREAS AND TO SUPPORT THESE FIELD OPERATIONS WITH EXISTING EMERGENCY OPERATING CENTERS AND INFORMATION SYSTEMS TO THE EXTENT POSSIBLE.

AS PART OF A COORDINATED FEDERAL RESPONSE TO A MAJOR TERRORIST INCIDENT, FEMA WOULD DEPLOY AN EMERGENCY RESPONSE TEAM (ERT) TO THE SCENE, LED BY A SENIOR FEMA OFFICIAL (SFO). THE ERT WILL BE SUPPORTED BY AN EMERGENCY SUPPORT TEAM (EST) HEADED BY AN EST DIRECTOR. THE EST WILL OPERATE FROM THE FEMA EMERGENCY INFORMATION AND COORDINATION CENTER (EICC) IN THE FEMA HEADQUARTERS IN WASHINGTON, D.C. THE SFO WILL BE APPOINTED BY THE DIRECTOR, FEMA, AND WILL COMMUNICATE AND PROVIDE INFORMATION AND REPORTS THROUGH THE EST USING THE OPERATIONAL FACILITIES OF FEMA.

TO SUPPORT THE SFO AND THE FEDERAL RESPONSE CENTER, FEMA HAS DEVELOPED AN INTEGRATED NATIONAL EMERGENCY MANAGEMENT SYSTEM (NEMS) THAT IS CAPABLE OF SUPPORTING THE FULL RANGE OF INFORMATION REQUIREMENTS IN EVERY PHASE AND TYPE OF ACTIVITY ASSOCIATED WITH EMERGENCY MANAGEMENT. NEMS PROVIDES AN OVERALL NATIONWIDE CAPABILITY TO SUPPORT EMERGENCY MANAGEMENT DECISION MAKING AT THE HIGHEST LEVELS OF GOVERNMENT THROUGH VARIOUS INFORMATION PROCESSING AND COMMUNICATION NETWORKS AS EMERGENCY SITUATIONS DICTATE. IT ALSO PROVIDES FOR INTERCONNECTIVITY WITH SYSTEMS OF THE WHITE HOUSE, DEPARTMENT OF STATE, DEPARTMENT OF DEFENSE, AND OTHER FEDERAL, STATE AND LOCAL SYSTEMS HAVING NATIONAL EMERGENCY FUNCTIONS. IT CONSISTS OF THE PHYSICAL FACILITIES, TELECOMMUNICATIONS, AND INFORMATION SYSTEMS REQUIRED FOR FEMA'S VITAL MANAGEMENT MISSION. INITIAL TELECOMMUNICATIONS SUPPORT WILL CONSIST OF FEMA'S FIXED AND MOBILE CAPABILITIES.

AS PART OF OUR MOBILIZATION PREPAREDNESS, RESOURCES ASSESSMENT EFFORTS, FEMA WORKS CLOSELY WITH OTHER DEPARTMENTS AND AGENCIES IN THE DEVELOPMENT AND SHARING OF EMERGENCY MANAGEMENT DATA BASES AND AUTOMATED MODELING CAPABILITY WHICH SUPPORT INDUSTRIAL MOBILIZATION PLANNING. DURING 1988, FEMA SPONSORED TWO DATA BASE AND MODELING WORKSHOPS TO PROMOTE CLOSER RELATIONSHIPS AMONG EMERGENCY MANAGEMENT ORGANIZATIONS IN THE FEDERAL STRUCTURE AND THE CIVIL SECTOR. THIS DATA IS USED TO ASSIST EMERGENCY MANAGERS TO MONITOR OUR STATE OF READINESS AND TO ASSURE CONTINUED PRODUCTION CAPABILITY IN A NATIONAL SECURITY EMERGENCY. IT IS ALSO USED TO DEVELOP PROJECTIONS, ANALYSES, AND OPTIONS TO SUPPORT THE DECISION-MAKING PROCESS FOR POLICIES AND PROGRAMS TO AVAIL ESSENTIAL RESOURCES FOR MILITARY AND CIVILIAN MOBILIZATION NEEDS IN MAJOR DOMESTIC DISASTERS AND NATIONAL SECURITY EMERGENCY SITUATIONS. IN THE EVENT OF TERRORIST ACTS, RESULTING IN A DISRUPTION ON A POTENTIAL PORTION OF NEW YORK CITY'S "HIGH TENSION ELECTRIC POWER GRID", FEMA WOULD RELY ON THE DEPARTMENT OF ENERGY TO PROVIDE SPECIFIC INFORMATION ON THE NATURE OF THE DISRUPTION, ITS LIKELY IMPACT, AND STEPS NECESSARY FOR RESTORATION OF ELECTRICAL SERVICE. HOWEVER, TO FACILITATE ASSESSMENT AND RESTORATION ACTIVITIES, FEMA WOULD BE ABLE, USING THE INTEGRATED EMERGENCY MANAGEMENT INFORMATION SYSTEM (IEMIS) AND THE INTEGRATED MANAGEMENT AND ECONOMIC AND ANALYSIS SYSTEM (IMEASY), TO DEVELOP AND DISPLAY MAPPING, GRAPHICS AND

ANALYTICAL DATA IDENTIFICATION OF INDUSTRIAL CAPACITY LOST AND THE NUMBER OF PEOPLE WITHOUT POWER. IF THE DISRUPTION SHOULD LAST FOR AN EXTENDED PERIOD OF TIME, FEMA WOULD BE ABLE TO IDENTIFY SUPPORT, I.E., HEAT, FOOD, WATER, THE AFFECTED POPULATION NEEDS.

LET ME TURN NOW TO SOME OF THE OTHER THINGS FEMA IS DOING TO ENHANCE THE NATION'S CAPABILITY TO RESPOND TO THE CONSEQUENCES OF HIGH-TECHNOLOGY TERRORISM.

INTERAGENCY NUCLEAR, BIOLOGICAL AND CHEMICAL TERRORISM RESPONSE PLANNING

FEMA IS A MEMBER OF THE NUCLEAR, BIOLOGICAL AND CHEMICAL, (NBC) WORKING GROUP OF THE INTERDEPARTMENTAL GROUP ON TERRORISM (IG/T). THIS GROUP IS EXAMINING OUR GOVERNMENT'S CAPACITY TO RESPOND TO NBC THREATS, AND WORKING ON PLANS, PROCEDURES AND CAPABILITY TO RESPOND TO CHEMICAL AND BIOLOGICAL TERRORIST INCIDENTS. THE NBC WORKING GROUP HAS ALSO DEVELOPED AN ACTIVE PROGRAM OF EXERCISES TO TEST RESPONSE CAPABILITY. VARIOUS EXERCISES HAVE INVOLVED THE FEDERAL GOVERNMENT ALONE, THE FEDERAL GOVERNMENT COORDINATING WITH STATE AND LOCAL GOVERNMENTS, AND THE FEDERAL GOVERNMENT ACTING WITH OTHER COUNTRIES. OTHER FEMA COMMITTEE PARTICIPATION ACTIVITIES INCLUDE:

- IG/T, EXERCISE COMMITTEE
- NUCLEAR EMERGENCY SEARCH TEAM (NEST), OPERATIONS WORKING GROUP
- NEST, DAMAGE LIMITATION WORKING GROUP
- CHEMICAL/BIOLOGICAL INCIDENT RESPONSE RESEARCH AND DEVELOPMENT SUBGROUP
- NATIONAL DISASTER MEDICAL SYSTEM EXERCISE COMMITTEE

INTERAGENCY ENERGY ACTIVITIES

FEMA IS A MEMBER OF THE INTERAGENCY GROUP ON ENERGY VULNERABILITY (IG-EV). THE MISSION OF THE IG-EV IS TO EXAMINE THE VULNERABILITY OF U.S. ENERGY SYSTEMS, AND TO PREPARE OPTIONS TO REDUCE THIS VULNERABILITY OR TO MITIGATE THE IMPACTS OF DISRUPTION TO ENERGY SYSTEMS. U.S. ENERGY SYSTEMS INCLUDE: ELECTRIC POWER, CRUDE OIL AND PETROLEUM PRODUCTS (IMPORTS, PRODUCTION, REFINING, DISTRIBUTION), NATURAL GAS AND COAL.

THE DEPARTMENT OF ENERGY AND FEMA HAVE COLLABORATED ON A NUMBER OF ACTIVITIES WHOSE PURPOSES ARE THE MITIGATION AND MANAGEMENT OF NATURAL GAS SYSTEM EMERGENCIES. AT THE PRESENT TIME, WE ARE JOINTLY DEVELOPING THE FOLLOWING: (1) A NATURAL GAS OUTREACH INITIATIVE; (2) A PILOT SECURITY PLANNING PROGRAM

FOR THE SIXTH ARMY AREA; (3) A SCOPING STUDY CONCERNING THE NATURE AND EXTENT OF INTERDEPENDENCE AND INTERRELATIONSHIPS BETWEEN TELECOMMUNICATIONS AND THE ELECTRIC POWER NETWORK; AND (4) A PILOT STUDY OF SAN DIEGO AND LOS ANGELES THAT RELATES DEFENSE INTERESTS TO ENERGY SUPPLY.

FEMA IS A MEMBER OF THREE WORKING GROUPS CREATED TO SUPPORT THE IG-EV. THE ENERGY VULNERABILITY ASSESSMENT SUBGROUP (EVAS); DATABASE AND PROJECTIONS SUBGROUP AND THE RESPONSE DEVELOPMENT SUBGROUP. FEMA ALSO PARTICIPATES ALONG WITH THE DEPARTMENT OF DEFENSE AND THE NATIONAL COMMUNICATIONS SYSTEM IN AN EVAS WORKING GROUP (WG) THAT IS DEVELOPING ANALYTICAL TECHNIQUES TO BE USED BY GOVERNMENT AND INDUSTRY FOR BETTER ASSESSING ENERGY SYSTEM VULNERABILITIES ON A NATIONAL SCALE.

WE ARE ASSISTING THE IG-EV TO OBTAIN MAXIMUM BENEFIT BY LOOKING AT INFRASTRUCTURE SYSTEMS IN TERMS OF THEIR VULNERABILITY TO A REGIONAL OR NATIONAL LEVEL OUTAGES. TOWARD THIS END, FEMA HAS HELPED SPONSOR THE DEVELOPMENT OF COMPUTER-AIDED DELPHI METHODOLOGIES THAT CAN BE USED TO MITIGATE THESE KIND OF DISRUPTIONS.

OTHER INTERAGENCY AND JOINT INDUSTRY-GOVERNMENT ACTIVITIES

THE WORK OF SEVERAL OTHER INTERAGENCY AND JOINT INDUSTRY-GOVERNMENT GROUPS CURRENTLY ADDRESSING MOBILIZATION ISSUES AND PROBLEMS MAY HAVE SIGNIFICANCE IN TERRORIST INCIDENTS WITH NATIONAL IMPACT.

THE NATIONAL MOBILIZATION INTERAGENCY GROUP (NMIG) IS PART OF THE CURRENT INTERAGENCY NATIONAL SECURITY EMERGENCY PREPAREDNESS SYSTEM. THE NMIG IS COMPOSED OF REPRESENTATIVES AT THE ASSISTANT SECRETARY LEVEL FROM THE MAJOR DEPARTMENT AND AGENCIES IN THE FEDERAL GOVERNMENT THAT WOULD HAVE A SIGNIFICANT ROLE IN RESPONDING TO A SCENARIO OF EVENTS LIKE A MAJOR ELECTRIC POWER OUTAGE.

THE NMIG CONTAINS VARIOUS SUBGROUPS WHICH ADDRESS SPECIFIC ISSUES WITHIN THE MOBILIZATION ARENA: 1) THE ECONOMIC AFFAIRS SUBGROUP DEALS WITH THE ECONOMIC AND FINANCIAL POLICY ASPECTS OF A MOBILIZATION; 2) THE MOBILIZATION READINESS SUBGROUP ADDRESSES POLICIES AND PROCEDURES FOR MOBILIZING U.S. INDUSTRY DURING AN EMERGENCY; 3) THE STANDBY AUTHORITIES SUBGROUP EXAMINES EMERGENCY AUTHORITIES NEEDED FOR A NATIONAL SECURITY EMERGENCY; AND 4) THE

ORGANIZATIONAL IMPLEMENTATION SUBGROUP ADDRESSES WAYS TO EFFECTIVELY ORGANIZE THE GOVERNMENT RESPONSE TO EMERGENCIES.

IN JANUARY, 1986, A JOINT INDUSTRY GOVERNMENT WORKING GROUP WAS ESTABLISHED TO LOOK AT IMPORTANT ISSUES IN TELECOMMUNICATIONS INDUSTRY MOBILIZATION (TIM).

THE TIM GROUP IS COMPRISED OF REPRESENTATIVES FROM TELECOMMUNICATIONS MANUFACTURERS AND CARRIERS AND OF GOVERNMENT REPRESENTATIVES FROM THE DEPARTMENT OF COMMERCE, DEFENSE AND JUSTICE, THE GENERAL SERVICES ADMINISTRATION AND FEMA. THE GROUP IS CO-CHAIRED BY THE NATIONAL COMMUNICATION SYSTEM AND THE TELECOMMUNICATIONS INDUSTRY.

FOR THE PAST YEAR, THE TIM GROUP HAS FOCUSED ON SEVEN ISSUES:

- PERSONNEL STATUS, PROTECTION, AND RELOCATION
- MAINTENANCE OF STOCKPILES AND INVENTORIES
- DEPENDENCE ON FOREIGN SOURCES
- GOVERNMENT AND INDUSTRY MOBILIZATION MANAGEMENT STRUCTURE
- DEPENDENCE ON OTHER INFRASTRUCTURE SYSTEMS (ELECTRICITY, TRANSPORTATION, ETC.)
- TELECOMMUNICATIONS SERVICE SURGE REQUIREMENTS
- JURISDICTIONAL ISSUES (FEDERAL, STATE, LOCAL)

FINAL REPORTS ON THE FIRST FOUR ISSUE AREAS HAVE BEEN COMPLETED AND WORK IS CONTINUING ON THE LAST THREE ISSUE AREAS.

IN LATE JUNE, FEMA HOSTED AN INTERAGENCY MEETING ON PREPAREDNESS FOR WATER SUPPLY EMERGENCIES WITH THE U.S. ARMY CORP OF ENGINEERS (USACOE), ENVIRONMENTAL PROTECTION AGENCY (EPA), DEPARTMENT OF ENERGY (DOE), AND THE U.S. GEOLOGICAL SURVEY (USGS). THE MEETING WAS REQUESTED BY THE WATER, SCIENCE AND TECHNOLOGY BOARD OF THE NATIONAL RESEARCH COUNCIL. THE MEETING FOCUSED ON THE VULNERABILITY OF PUBLIC WATER SUPPLY SYSTEMS AND THE NEED TO IMPROVE OUR PREPAREDNESS FOR RESPONDING TO DISRUPTIVE EMERGENCIES AND ON NATIONAL SECURITY EMERGENCIES AND THE RESPECTIVE DEPARTMENTS AND AGENCIES ROLES AND RESPONSIBILITIES. WE ARE WORKING CLOSELY WITH THESE AGENCIES AND THE COUNCIL'S WATER SCIENCE AND TECHNOLOGY BOARD TO PURSUE WATER PLANNING WITHIN THE CONTEXT OF NATIONAL SECURITY EMERGENCY PREPAREDNESS.

HAVING MENTIONED HOW WE DEAL WITH THE PHYSICAL CONSEQUENCES OF TERRORISM WE WOULD LIKE TO NOTE FEMA'S INVOLVEMENT WITH THE DEPARTMENT OF DEFENSE'S KEY ASSET PROTECTION PROGRAM (KAPP). THE OBJECTIVE OF THIS PROGRAM IS TO DEVELOP AND PROMOTE THE SECURITY OF KEY ASSETS WITHIN THE U.S. TERRITORIES AND POSSESSIONS BY PROVIDING TO THE OWNERS OR MANAGERS OF SUCH ASSETS APPROPRIATE ADVICE, GUIDANCE AND PLANNING ASSISTANCE CONCERNING THE APPLICATION OF PHYSICAL SECURITY AND EMERGENCY PREPAREDNESS MEASURES.

IMPLEMENTATION OF THIS PROGRAM INCLUDING THE COMPILATION OF THE KEY ASSET LIST HAS BEEN DELEGATED TO THE U. S. FORCES COMMAND (FORSCOM) AT FORT MCPHERSON, GA. WE NOTE THAT MILITARY FACILITIES ARE NOT INCLUDED ON THE LIST. PROTECTION OF THESE FACILITIES IS THE RESPONSIBILITY OF THE RESPECTIVE MILITARY COMMANDERS.

FEMA'S INVOLVEMENT IN THIS PROGRAM STEMS FROM A MEMORANDUM OF AGREEMENT SIGNED AUGUST 15, 1988, IN WHICH FEMA HAS AGREED TO COORDINATE NOMINATIONS FOR THE KEY ASSET LIST FROM OTHER FEDERAL AGENCIES AND PROVIDE THIS INPUT TO FORSCOM.

AS A RELATED MATTER, WE WOULD LIKE TO CALL YOUR ATTENTION TO A LETTER THE DIRECTOR SENT TO THE ATTORNEY GENERAL JULY 26, 1988, CALLING HIS ATTENTION TO THE SHIFT IN PHYSICAL SECURITY RESPONSIBILITIES CONTAINED IN THE REVISED E. O. 11490, AND RECOMMENDING THAT DEPARTMENT OF JUSTICE (DOJ) CHAIR AN INTERAGENCY GROUP WITH PLANNING/OVERSIGHT RESPONSIBILITY FOR THE ASSET PROTECTION PROGRAM. DOJ HAS SUBSEQUENTLY CONCURRED WITH THIS RECOMMENDATION AND DELEGATED THE RESPONSIBILITY TO THE FBI.

WITH RESPECT TO DEALING WITH THE PHYSICAL CONSEQUENCES OF TERRORISM, TITLE I OF THE DEFENSE PRODUCTION ACT, PRIORITIES SUPPORT CAN BE AUTHORIZED TO OBTAIN THE NEEDED MATERIALS AND EQUIPMENT TO HELP RESTORE THE ELECTRIC POWER SYSTEM.

NATIONAL EMERGENCY TRAINING CENTER (NETC)

NETC SERVES AS A NATIONAL FOCAL POINT FOR THE DEVELOPMENT AND DELIVERY OF EMERGENCY MANGEMENT TRAINING TO ENHANCE EMERGENCY CAPABILITIES OF FEDERAL, STATE, AND LOCAL GOVERNMENTS AND THE PRIVATE SECTOR. THE NETC CAMPUS OFFERS A UNIQUE OPPORTUNITY TO BRING TOGETHER SENIOR EXPERTS FROM THE U.S. AND

ABROAD TO EXAMINE CRITICAL EMERGENCY MANAGEMENT PROBLEMS. THIS SHARING OF INFORMATION AND OPERATING PRACTICES BETWEEN THE LAW ENFORCEMENT COMMUNITY (FEDERAL, STATE AND LOCAL), THE FIRE SERVICES, EMERGENCY MEDICAL SERVICES AND CIVIL EMERGENCY PLANNERS IS PARTICULARLY GERMANE TO CATASTROPHIC CONSEQUENCES OF A TERRORIST ACT. OF PARTICULAR NOTE IN OUR TRAINING WORK IS THE OPPORTUNITY FOR PRACTICAL EXERCISES (CONSEQUENCES OF TERRORISM, HAZARDOUS MATERIALS, NUCLEAR POWER PLANT INCIDENTS, ETC.) STRESSING HOW VARIOUS EMERGENCY MANAGEMENT SPECIALITIES AND LEVELS OF GOVERNMENT AND THE PRIVATE SECTOR CAN AND SHOULD WORK TOGETHER.

IN CLOSING, FEMA'S AUTHORITIES HAVE PROVIDED A STRONG BASIS FOR THE AGENCY'S ACTIVITIES TO PLAN FOR, RESPOND TO, AND COORDINATE EFFORTS TO MITIGATE THE CONSEQUENCES OF A CATASTROPHIC TERRORIST INCIDENT. THE AGENCY'S RESPONSIBILITIES IN MOBILIZATION PLANNING IN RESPONSE AND ASSISTANCE TO VICTIMS OF DISASTERS AND IN THE BUILDING OF EMERGENCY MANAGEMENT CAPABILITIES AT ALL LEVELS ARE IMPORTANT ELEMENTS IN THE NATION'S ABILITY TO DEAL WITH THE CONSEQUENCES OF TERRORISM.

Senator **Leahy**. Thank you very much.

Let us—I am sorry, Mr. Alderman.

Mr. **Alderman**. Mr. Chairman, equal time, if I might. [Laughter.]

Senator **Leahy**. I am sorry, Mr. Alderman. Obviously, we are not going alphabetically here and I do want the Department of Defense to have a shot in here, no pun intended.

STATEMENT OF CRAIG ALDERMAN, JR.

Mr. **Alderman**. Thank you. It is a unique opportunity to be last in any roster, sir.

I am responsible in the Department of Defense for the development of policies, for guidance and oversight of the plans that implement those policies, and for military support to civil authorities in peace as well as in war time.

I have submitted to you a formal statement, which I would ask be entered in the record.

Senator **Leahy**. It will be.

Mr. **Alderman**. I am just going to hit two or three high points here before we turn it back over to you for discussion of the individual incidents.

My Department's policies and planning for coping with domestic incidents are founded on adherence to the principles of separation between the military and civil law enforcement and to the subjection of military power to civil control.

Now, I grant you that distinction may seem obscure to the general public if terrorists who are covertly sponsored by a foreign power, in fact, are operating on United States soil. But this committee is well aware of the primacy of civil law enforcement and our judicial system being fundamental to our Government and our society, and that the role of the military therefore can only be that of secondary support at the request of the civil authorities when the law enforcement needs or the humanitarian needs exceed the capabilities of those authorities.

I want to introduce briefly the specific roles and missions of my Department in this arena. First, in the most obvious area of support to civil law enforcement, the military responsiveness with materiel and equipment, technical advice, and forces is well coordinated, even while we do maintain the legalities of civil primacy.

We have procedures, we have plans, and we have years of practice in assisting both Federal law enforcement and that of the States. This assistance is provided through mechanisms by which the President may authorize military assistance in response to a formal request from any State.

In addition, we assist in covering both civil disturbances and counterterrorism, which is coordinated for all military departments and DOD components by the Secretary of the Army as the executive agent of the Secretary of Defense.

Now, second, the Secretary of the Army, in addition to that responsibility, is the executive agent for the Department of Defense for providing logistical and life-saving support to civil authorities faced with any form of disaster, whether it be man-made or natural.

Under the conditions of the Disaster Relief Act, when the President has declared a major disaster we are empowered to commit DOD resources in support of the amelioration of the effects of that disaster.

Additionally, in those emergencies in which immediate action by a military commander can assist the authorities in saving human life or protecting Government property by immediate response, the military does not have to wait for higher authority to give approval.

Third, we have a longstanding and effective procedure for obtaining a decision by the Secretary of Defense rapidly to apply DOD funds for emergency assistance to civil authorities, if necessary, prior to the declaration of a major disaster.

These kinds of requests are generally received either by the National Military Command Center or by the Secretary of Defense or one of the assistants. They are passed to the executive secretary for the Secretary of Defense, who processes them and approves them for the Secretary; and things begin to function right there.

In terms of resources that we can bring to bear [in addition to those which everybody normally thinks of as being associated with DOD of food, clothing, communications, transportation, and law enforcement assistance], the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict exercises policy oversight of special operation forces which may be employed under a variety of scenarios. Those may range from a general war to low-intensity conflict, and may include response to international terrorism.

Generally, this focus is outside the continental United States. In the absence of open or armed hostilities or warfare inside the United States, it would be a rare and extreme circumstance that would lead to the employment of a U.S. Department of Defense counterterrorism or other special operation force within the United States.

We have done this in the past and we undoubtedly will do it in the future, but it is not the norm. When it is done, it is done under the legal construct, again, of military support to civil law enforcement agencies.

Senator **Leahy**. What is an example of one time when you have done it, or is that something that would not be in open——

Mr. **Alderman**. No; we provided support, which I will not go into detail, during the prison uprisings in the past few months.

Senator **Leahy**. OK.

Mr. **Alderman**. I am capable of giving additional information in a closed hearing on that.

Senator **Leahy**. I understand.

Mr. **Alderman**. Second, sir, the assistant to the Secretary of Defense for Atomic Energy has general oversight of a number of highly specialized technological capabilities of our Department which can be made available to assist civil authorities in the nuclear, biological, or chemical hazard area.

I would like to say that I have with me here this morning not only representatives of my staff, but a representative from the Department of the Army as the executive agent for most of these types of actions, a representative from the Office of the Assistant

Secretary of Defense for Special Operations and Low-Intensity Conflict, and a representative from the Assistant to the Secretary of Defense for Atomic Energy.

I also have brought a representative from the general counsel, mindful that there are legal minefields out here as well as procedural minefields.

We are available to answer general questions or specific questions, sir.

[The statement of Mr. Alderman follows:]

INTRODUCTORY REMARKS FOR THE DEPARTMENT OF DEFENSE

MR. CRAIG ALDERMAN, JR.

DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY

MR. CHAIRMAN, I AM CRAIG ALDERMAN, JR., DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY. I AM RESPONSIBLE FOR THE DEVELOPMENT OF POLICIES, AND FOR GUIDANCE AND OVERSIGHT FOR PLANS AND PROCEDURES, BY WHICH THE DEPARTMENT OF DEFENSE PROVIDES MILITARY SUPPORT TO CIVIL AUTHORITIES PEACE AND IN WAR.

THEREFORE, AS A GENERAL INTRODUCTION FOR OUR CONTRIBUTION TO YOUR INQUIRY, I WILL ADDRESS THE CAPABILITIES OF THE DEPARTMENT OF DEFENSE WITHIN THE CONTEXT OF THAT INQUIRY INTO

> "HOW THE EXECUTIVE BRANCH IS STRUCTURED, EQUIPPED AND PREPARED TO DEAL WITH TERRORIST ATTACKS ON THE UNITED STATES USING OR AIMED AT ADVANCED TECHNOLOGIES..., AND
>
> "...WHAT MECHANISMS EXIST TO COOPERATE AND COORDINATE IN CRISIS MANAGEMENT,...TO INTERACT WITH STATE AND LOCAL GOVERNMENT AND LAW ENFORCEMENT,...AND
>
> "...WHICH AGENCIES ARE RESPONSIBLE FOR WHAT ASPECTS OF COUNTERTERRORISM POLICY AND IMPLEMENTATION."

THE DEFENSE DEPARTMENT'S POLICIES AND PLANNING ARE FOUNDED ON OUR ADHERENCE TO THE SEPARATION BETWEEN THE MILITARY AND CIVIL LAW ENFORCEMENT. AND TO THE SUBJECTION OF MILITARY POWER TO CIVILIAN CONTROL. WHILE THAT DISTINCTION MAY SEEM OBSCURE TO THE GENERAL PUBLIC IF TERRORISTS WHO ARE COVERTLY SPONSORED BY A FOREIGN POWER ARE OPERATING ON U.S. SOIL, THIS COMMITTEE IS WELL AWARE THAT THE PRIMACY OF CIVIL LAW ENFORCEMENT AND THE JUDICIAL SYSTEM IS FUNDAMENTAL TO OUR GOVERNMENT AND SOCIETY, AND THAT THE ROLE OF THE MILITARY CAN ONLY BE

THAT OF SECONDARY SUPPORT, AT THE REQUEST OF CIVIL AUTHORITIES, WHEN LAW ENFORCEMENT NEEDS EXCEED CAPABILITIES.

I, THEREFORE, WANT TO INTRODUCE BRIEFLY THE SPECIFIC ROLES AND MISSIONS OF THE DEPARTMENT OF DEFENSE IN PROVIDING MILITARY SUPPORT TO CIVIL AUTHORITIES, AND OUR RELATIONSHIPS TO OTHER EXECUTIVE BRANCH AGENCIES, AS A PRECEDENT FOR OUR ANSWERS TO YOUR QUESTIONS AND DISCUSSION OF THE SCENARIOS YOU HAVE POSED.

FIRST, IN THE MOST OBVIOUS ARENA OF SUPPORT TO CIVIL LAW ENFORCEMENT, THE MILITARY RESPONSIVENESS WITH MATERIEL AND EQUIPMENT, TECHNICAL ADVICE, AND FORCES IS WELL COORDINATED, EVEN WHILE MAINTAINING THE LEGALITIES OF CIVIL PRIMACY. WE HAVE PROCEDURES, PLANS AND YEARS OF PRACTICAL EXPERIENCE IN ASSISTING BOTH FEDERAL LAW ENFORCEMENT, THROUGH THE LEADERSHIP OF THE DEPARTMENT OF JUSTICE (INCLUDING THE FEDERAL BUREAU OF INVESTIGATION); AND THE STATES. THAT ASSISTANCE IS PROVIDED THROUGH MECHANISMS BY WHICH THE PRESIDENT MAY AUTHORIZE MILITARY ASSISTANCE (WITH OVERSIGHT FROM THE DEPARTMENT OF JUSTICE) IN RESPONSE TO A FORMAL REQUEST FROM ANY STATE. THAT SUPPORT, WHICH WE MANAGE UNDER A SYSTEM COVERING BOTH CIVIL DISTURBANCES AND COUNTERTERRORISM, IS COORDINATED FOR ALL MILITARY DEPARTMENTS AND DOD COMPONENTS BY THE SECRETARY OF THE ARMY AS EXECUTIVE AGENT FOR THE SECRETARY OF DEFENSE.

ADDITIONALLY, THE SECRETARY OF THE ARMY IS THE EXECUTIVE AGENT FOR THE SECRETARY OF DEFENSE FOR PROVIDING LOGISTICAL AND LIFE SAVING SUPPORT TO CIVIL AUTHORITIES FACED WITH ANY FORM OF DISASTER. IN THE RELATIVELY STRAIGHTFORWARD SITUATIONS OF NATURAL AND TECHNOLOGICAL CONDITIONS FOR WHICH THE PRESIDENT HAS DECLARED A MAJOR DISASTER UNDER THE DISASTER RELIEF ACT, THE DEPARTMENT OF DEFENSE IS IMMEDIATELY ABLE TO SUPPORT A FEDERAL CIVIL GOVERNMENT RESPONSE THAT NORMALLY IS COORDINATED BY THE FEDERAL EMERGENCY MANAGEMENT AGENCY. FURTHER, IN THOSE EMERGENCIES IN WHICH IMMEDIATE ACTION BY A MILITARY

COMMANDER CAN ASSIST CIVIL AUTHORITIES IN SAVING HUMAN LIFE OR PROTECTING FEDERAL GOVERNMENT FUNCTIONS OR PROPERTY, THE MILITARY AND OTHER DOD AGENCIES ARE AUTHORIZED TO RESPOND WITHOUT PRIOR APPROVAL OF FUNDING.

FINALLY, WE HAVE A LONGSTANDING AND EFFECTIVE PROCEDURE FOR OBTAINING A DECISION BY THE SECRETARY OF DEFENSE TO APPLY DOD FUNDS FOR EMERGENCY ASSISTANCE TO CIVIL AUTHORITIES, IF NECESSARY PRIOR TO A PRESIDENTIAL DECLARATION OF EMERGENCY. SUCH EMERGENCY REQUESTS ARE RECEIVED DIRECTLY BY THE EXECUTIVE SECRETARY TO THE SECRETARY OF DEFENSE (OR PASSED TO THE EXECUTIVE SECRETARY IF RECEIVED BY OTHERS), AND EMERGENCY AUTHORIZATIONS ON BEHALF OF THE SECRETARY THEN ARE PASSED TO ANY APPROPRIATE DOD AGENCY. THOSE DECISIONS OFTEN ARE IMPLEMENTED ON A JOINT SERVICE BASIS THROUGH THE EXECUTIVE AGENCY OF THE SECRETARY OF THE ARMY WITHIN THE 48 CONTIGUOUS STATES, AND BY THE COMMANDER IN CHIEF, U.S. PACIFIC COMMAND FOR HAWAII AND THE PACIFIC TERRITORIES, BY THE COMMANDER OF THE ALASKAN AIR COMMAND FOR ALASKA, AND BY THE COMMANDER IN CHIEF, U.S. ATLANTIC COMMAND FOR PUERTO RICO AND THE VIRGIN ISLANDS.

THE ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW INTENSITY CONFLICT EXERCISES POLICY OVERSIGHT OF SPECIAL OPERATIONS FORCES, WHICH MAY BE EMPLOYED UNDER A VARIETY OF SCENARIOS, RANGING FROM SUPPORT OF GENERAL WAR EFFORTS TO LOW INTENSITY CONFLICT SITUATIONS, WHICH MAY INCLUDE RESPONSE TO INTERNATIONAL TERRORISM. IN THE ABSENCE OF OPEN, ARMED HOSTILITIESOR WARFARE IN THE UNITED STATES, ONLY A RARE AND EXTREME CIRCUMSTANCE WOULD LEAD TO EMPLOYMENT OF ANY UNITED STATES COUNTERTERRORISM OR OTHER SPECIAL OPERATIONS FORCES WITHIN THE UNITED STATES; AND, EVEN IN THOSE CIRCUMSTANCES, THE FORCES WOULD BE EMPLOYED ONLY IN THE LEGAL POSTURE OF PROVIDING MILITARY ASSISTANCE TO CIVIL LAW ENFORCEMENT AT CIVIL REQUEST.

THE ASSISTANT TO THE SECRETARY OF DEFENSE FOR ATOMIC ENERGY HAS GENERAL OVERSIGHT OF A NUMBER OF HIGHLY SPECIALIZED TECHNOLOGICAL CAPABILITIES OF THE DEPARTMENT OF DEFENSE AGENCIES, WHICH CAN BE MADE AVAILABLE TO ASSIST CIVIL AUTHORITIES IN RESPONSE TO NUCLEAR, BIOLOGICAL OR CHEMICAL HAZARDS. IN MOST OF THOSE EMERGENCY CONDITIONS, OTHER THAN EMERGENCIES ON MILITARY INSTALLATIONS OR DEALING WITH MILITARY WEAPONS, THE TOTAL FEDERAL GOVERNMENT RESPONSE TO ACTUAL OR POTENTIAL CATASTROPHE WOULD BE ADDRESSED BY FEDERAL INTERAGENCY ORGANIZATIONS UNDER THE LEAD OF THE DEPARTMENT OF ENERGY, THE FEDERAL EMERGENCY MANAGEMENT AGENCY, OR THE FBI, WITH DOD ONLY FURNISHING TECHNICAL ADVICE AND ASSISTANCE AS APPROPRIATE. AGAIN, MANY OF THE OPERATIONS FOR THE ACTUAL DEPLOYMENT OF TECHNOLOGICAL SUPPORT TEAMS FALL UNDER THE EXECUTIVE AGENCY OF THE SECRETARY OF THE ARMY I HAVE DISCUSSED EARLIER.

BEFORE WE ALL RESPOND TO YOUR QUESTIONS, I WOULD LIKE TO MENTION ONE SPECIFIC DOD PROGRAM AND ONE GENERIC CAPABILITY WHICH BEAR INDIRECTLY ON THE TOPIC AT HAND.

THE DOD KEY ASSET PROTECTION PROGRAM (KAPP) IS A BASIS FOR OUR PLANNING TO ASSIST CIVIL LAW ENFORCEMENT AUTHORITIES IN THE PROTECTION OF CERTAIN CIVILIAN-OWNED FACILITIES THAT HAVE BEEN IDENTIFIED AS CRITICAL TO DOD'S ABILITY TO MOBILIZE, DEPLOY OR SUSTAIN OUR MILITARY FORCES IN A NATIONAL SECURITY EMERGENCY. THE LIST ITSELF IS CLASSIFIED, AND ONLY IN ITS SECOND YEAR OF CONTINUOUS DEVELOPMENT. THE PROCESS OF MILITARY PLANNING WITH THE CIVIL SECTOR WITH RESPECT TO INDIVIDUAL FACILITIES IS DEVELOPING UNDER THE LEADERSHIP OF THE COMMANDER IN CHIEF, FORCES COMMAND, FOR THE 48 CONTIGUOUS STATES, AND THE COMMANDERS MENTIONED EARLIER FOR THE REMAINDER OF THE UNITED STATES. HOWEVER, THAT PLANNING PROCESS EMPHASIZES THE DEVELOPMENT OF A MILITARY CAPABILITY AT THE GRASS ROOTS LEVEL, WHICH MAY PROVE IN TIME TO BE THE MOST EFFECTIVE MILITARY CONTRIBUTION TO PEACETIME DETERRENCE OF, AND RESPONSE TO, TERRORIST ATTACKS ON TECHNOLOGICAL TARGETS IN THE UNITED STATES.

KEY ASSET PROTECTION PLANS WILL BE DEVELOPED BY THE ARMY NATIONAL GUARD STATE AREA COMMAND (STARC) FOR EACH STATE, IN COORDINATION WITH THE OWNERS OF THE FACILITIES AND THE CIVIL LAW ENFORCEMENT AGENCIES HAVING JURISDICTION. I EMPHASIZE, HOWEVER, THAT, THESE PLANS ARE DEVELOPED AS CONTINGENCY PLANS FOR NATIONAL SECURITY EMERGENCIES OR WAR; AND, PRIOR TO MOBILIZATION OF THE NATIONAL GUARD, THEY WOULD NOT BE IMPLEMENTED UNDER THE AUTHORITY OF THE DEPARTMENT OF DEFENSE.

THE EQUIPMENT, TRAINING AND ADMINISTRATION OF THE NATIONAL GUARD UNDER AUSPICES OF THE DEPARTMENTS OF THE ARMY AND AIR FORCE IS CRITICALLY IMPORTANT TO THE THE NATIONAL DEFENSE; AND THE MAJORITY OF OUR WARTIME CONTINGENCY PLANS ARE DEPENDENT ON THE TIMELY DEPLOYMENT OF THE NATIONAL GUARD UNITS. HOWEVER, IN THE EVENT OF PEACETIME TERRORIST ATTACKS ON U.S. SOIL, THE NATIONAL GUARD FORCES PROVIDE TO EACH STATE A VERY SUBSTANTIAL CAPABILITY FOR AUGMENTATION OF STATE AND LOCAL POLICE AND CIVIL DEFENSE RESOURCES. WE HAVE DESIGNED THE KEY ASSET PROTECTION PROGRAM WITH THE AWARENESS THAT PLANS MADE FOR IMPLEMENTATION BY ORDER OF THE SECRETARY OF DEFENSE UPON MOBILIZATION CAN BE EQUALLY EFFECTIVE FOR IMPLEMENTATION BY THE GOVERNORS UNDER OTHER CIRCUMSTANCES AND OTHER LEGAL AUTHORITIES, AND THAT PLANNING AND EXERCISES TO PROTECT SPECIFIC KEY ASSETS BUILD GENERIC CAPABILITIES FOR RESPONSE TO A WIDE RANGE OF POSSIBLE THREATS, INCLUDING TERRORISM.

TO CONCLUDE, THE DEPARTMENT OF DEFENSE MAINTAINS A BROAD RANGE OF CAPABILITIES FOR RESPONSE TO TECHNO-TERRORISM USING RADIOLOGICAL, CHEMICAL, BIOLOGICAL, OR CONVENTIONAL WEAPONS; AND FUTURE TECHNOLOGICAL DEVELOPMENTS ARE EXPECTED TO KEEP PACE WITH DEVELOPING THREATS. WITH THESE CAPABILITIES, WE ARE READYTO SUPPORT CIVIL AUTHORITIES FOR LAW ENFORCEMENT AND HUMANITARIAN MISSIONS, WHICH MAY BE UNDERTAKEN BY THE FEDERAL GOVERNMENT ALONE OR IN

CONJUNCTION WITH THE STATES. WE ALSO SUPPORT THIS COMMITTEE'S INITIATIVE TO REVIEW THE GOVERNMENT'S PREPAREDNESS FOR A COORDINATED AND EFFECTIVE RESPONSE TO ANY FORM OF POTENTIAL ATTACK ON THE UNITED STATES, WHICH WE VIEW AS A CRITICAL ELEMENT OF CIVIL DEFENSE AND OF OUR ABILITY TO EMPLOY THE NATION'S MILITARY POWER EFFICIENTLY DURING ANY NATIONAL SECURITY EMERGENCY.

THANK YOU.

Senator **Leahy**. Thank you. That is one of the reasons—those potential minefields—for making sure that each of you had received the copies of the various scenarios we are going to discuss here.

As I understand it, all we are discussing is taken from the public domain. We may have followup afterwards in either classified questions or in a classified session, but I think everything that we have here is something that can be done in open session.

Let us take the first illustrative scenario, the commercial airliner shootdown. That is where a Middle East terrorist group announces in Beirut that it has got five Stinger missiles and it is going to shoot down some American commercial aircraft inside the United States in retaliation for the downing of the Iranian airliner by the U.S.S *Vincennes*.

Now, the five Stinger missiles—that is a fairly realistic thing. There are so many of those floating around the world today that anybody with some money and a minimum of connections can get Stingers.

So, 2 weeks later, this same terrorist group announces in Beirut that within 1 week they will shoot down an American aircraft as the first of a series of actions. Then 3 days later, it does; it shoots down a small commuter flight with 12 passengers on it somewhere near a mid-sized city on the West Coast. Hit, run, boom, gone; nobody is arrested.

The next day, they announce in Beirut that their next target is going to be a large airliner, and 3 weeks later when a jumbo jet is flying into an airport in a major Midwestern city, they shoot it down with a Stinger, and at that time a couple of people get captured.

They reiterate that there are 3 more Stingers left and their people have those somewhere in the United States, without saying where, and they intend to use them. They do not care if they are caught and they become martyrs. In fact, I think, as we have found with some of the people who have been involved in terrorist attacks before, martyrdom becomes almost an extra advantage to them.

So, having done that and having this situation, what is the executive branch interagency mechanism that would come into place once a scenario like this started to unfold, Mr. Revell?

Mr. **Revell**. Well, obviously, our first concern is the verification and the authenticity of the threat, and there we would be relying primarily upon the intelligence community to authenticate through every means available to us to the greatest extent possible that this is, in fact, a valid threat and one that would require the activation of a substantial contingency response.

We have various means to do this. The intelligence community and the scientific and forensic community are able to assess the content of messages both from a psycho-linguistic behavioral science and forensic science capability, and that is all in place and has been utilized.

If we went forward and, of course, the threat was determined to be a real and valid threat, then we would go into an alert status. We have mechanisms available in the law enforcement community to put out a threat alert and threat assessment.

Then, since we are dealing with airports, we have in place, with airport and police authorities throughout the United States, contingency plans for dealing with hijacking and other crimes at airport facilities. Those procedures would be activated and we would be at each location across the country dealing with our counterparts at the State and local level and doing contingency planning.

Senator LEAHY. Well, at the point where the commuter flight is shot down and the terrorists announcing in connection with that—I mean, at that point it would be assumed that there really is no question the threat is real, and there is also no question that it is a Stinger missile. It is following exactly what they say.

The intelligence agencies, without going into the procedure they would follow—there is no question that there is a group out here with several Stingers, maybe five, maybe four, maybe six. Who knows? But there are a number of them out there. They have demonstrated their willingness to shoot down an aircraft.

There is absolutely no question about it. It is a very serious thing, and I am talking about the period before the major airliner gets shot down. Now, at that point is the FBI the lead agency in coordinating?

Mr. REVELL. Yes, sir.

Senator LEAHY. At some point, does the FAA—I mean, would this shift? Here we have one plane shot down. I do not know how many airports we have in this country, but certainly there must be over 500 to 1,000, or more commercial airports.

At some point, does it shift from the FBI to the FAA or anybody else?

Mr. REVELL. Not in dealing with the terrorist incidents themselves. Obviously, the FAA would be an integral part of the protection of the air transport system, and we would not in any way attempt to usurp that responsibility. We would not even have the capability to undertake that.

But we would still be the lead agency for attempting to identify the organization, the group, to locate them, and to obviously neutralize their activities through arrest and otherwise.

We would not be in the position of trying to determine what the air traffic changes would be. We would be working with local authorities on providing additional security, but that security would be the responsibility of the FAA and the airport authorities and the police. We do not get into the provision of protective resources. That is, of course, not our role.

But in this scenario, once, obviously, the threat has become a reality, we would also be doing something else. We would be asking for military support in assessing the potential of these weapons, how they can be detected, what their range is, what their capability is, and then putting that information into the system to enhance the protective capability at each of the airports where a threat would be determined to be a likelihood.

Senator LEAHY. The FBI is still the lead agency in this?

Mr. REVELL. For that process, yes, sir.

Senator LEAHY. Well, let us ratchet it up one more. These are not, I think we would all agree, implausible scenarios if somebody really wanted to go out and make a terrorist attack on the United States.

The terrorist infrastructure is there in a number of different terrorist groups. The weapons are available. The financing and some of the diplomatic cover necessary could be available if the decision is made.

So, we are up to the next step where a major airliner is shot down. Now, I would have to assume in a case like that that at this point there is growing panic around the country. I am sure there would be no question that at airports around the Nation, especially major airports—La Guardia, Dulles, O'Hare, LAX, and so on—they are going to have highly beefed-up security.

At this point, again, is the FBI still the lead?

Mr. REVELL. Well, the Attorney General, of course, is the ultimate——

Senator LEAHY. Right; I realize that.

Mr. REVELL. But we have the incident management responsibility, and unless, of course, the President determined that he would pull into the NSC or the NSPG that authority, it would continue to reside with the Attorney General and we would have the actual on-the-ground responsibility.

But this is not a singular responsibility, I have to continue to emphasize, because it is obviously not only an interagency, but an intergovernmental process. You would have governors and mayors that would be certainly involved in the entirety of this.

Senator LEAHY. Have you gamed out something like this?

Mr. REVELL. We have gamed out a number of serious terrorist scenarios. We have exercised aircraft hijacking. We have had actual cases of threat by missile against airliners and, of course, we have had a situation where we did detect explosive devices on board an Air India flight.

So we have exercised major scenarios. We have had real experience in something similar to these scenarios.

Senator LEAHY. Have you gone into the question of the psychological effect in this country, how it may affect our command and control, the question of whether we have to shift to alternative types of transportation, even the potential disruption of actually closing down major airports for a period of days or even weeks?

Mr. REVELL. No, sir.

Senator LEAHY. When a plane has been shot down, your law enforcement role, though, does not change. I mean, there is no plan that the Department of Justice would give up that role to DOD or FEMA or FAA or anybody else?

Mr. REVELL. No, sir; we would, of course, call upon the National Transportation Safety Board to assist us in the actual investigation at the site. Presumably, we would know immediately that it was an act of sabotage through the use of the Stinger, so the primacy of the law enforcement role would be established at the outset.

When we have a crash of a plane, we presume initially that it is not by sabotage and the National Transportation Safety Board has that responsibility. If we determine it was sabotage, that responsibility reverts to us as far as the lead responsibility.

Senator LEAHY. But you do not have in those plans what you would do to go to alternative transportation systems in this country or anything like that?

Mr. **Revell**. No, sir; we do not deal with the consequences of terrorism. That is FEMA and the Department of Energy and others. Our responsibility is to protect, plan for, and resolve, and then, of course, to provide any assistance we can to those agencies that must deal with the consequences.

Senator **Leahy**. Well, let me ask, then, Mr. Woloshyn, what about this: Is there some kind of a plan if something like this happens, how we would go to alternative transportation?

I would assume if a 747 gets shot down coming into a major city, it being the second one in a matter of weeks, and the news media broadcasts the fact that there are three more Stingers out there, while it might be easy to get a seat on otherwise overbooked airlines, there is going to be some reluctance to use them.

There is going to be sheer panic, actually, in this country and people are not about to travel. Has FEMA thought about that?

Mr. **Woloshyn**. Yes, we have, Mr. Chairman. The President, under the generic structure that I had made reference to, the national system for emergency coordination—the President may very well choose to select a national coordinator who would essentially be responsible for assuring that there is adequate coordination among the various departments and agencies.

Mr. Revell was entirely correct in asserting that the FBI would obviously have the lead in the beginning of the scenario and through all the law enforcement aspects and dealing with the various law enforcement components.

But at some point, as Mr. Revell also indicated, the lead responsibility for the transportation coordination aspects, for the problems of trying to find differing means of transportation, trying to identify what kind of rail lines may be beefed up in order to provide more rail transport, trying to determine what kind of regulations may have to be waived or issued in order to provide for pooling and busing service, and so on, for a population that may not be inclined to ride the airplanes under these circumstances—that problem would shift primarily to the Department of Transportation.

The Department of Transportation would then be in a position to work with other agencies. For example, DOD may have some transportation capability of its own that could be put on line to assist in providing for divergent or differing means of transportation.

There are data bases available. In fact, there are very large graphic digital display-type maps that, for example, would show the transportation network in the country, would show the roads and highway networks and the railroad transports.

Senator **Leahy**. And have you gamed that out with the Department of Transportation?

Mr. **Woloshyn**. We run a series of games. That particular scenario, I am not certain, Mr. Chairman, whether we have gamed that particular scenario. But we do run games in which there is a problem of backlogs and stoppages in transportation and what kind of divergent capabilities would be available, alternative capabilities, and we do run those kind of games.

Senator **Leahy**. You are also dealing with sheer panic here. It is not just a question of what happens if two or three major airports just get shut down because the Department of Defense or the FBI says that they cannot, based on the particular threat, guarantee security for at least a period of time, or need that period of time to be able to have that airport closed down while they concentrate security elsewhere. That could be a very realistic possibility. But beyond that, you go into questions of panic.

Mr. **Woloshyn**. You are entirely correct, Mr. Chairman. That would be a very important problem, and the way that would be handled at the Federal level would be essentially as a part of the emergency coordinating structure we would very early introduce Health and Human Services, the Public Health Service, other medical experts and other departments and agencies that have expertise in terms of dealing with public hysteria and public anxiety.

We would, under those circumstances, be setting up a joint information center. More than likely, there would be a center that would be available to communicate information through the media about alternative means of transportation, the prospects of injury or damage that may result from use of existing transportation.

We would try to allay public anxiety and concern by way of using the public media, as well as in some cases perhaps even using the Emergency Broadcast System to provide information to the public.

But this would be a largely coordinated effort. The FBI would be involved, obviously. The Department of Transportation would be involved, HHS would be involved, and other agencies that have specific expertise to lend would be involved.

We would be working very closely with the States and localities. We would, for example, through our regional network, be continuously sharing information with State emergency managers and providing a continuing source of information to them so that they can take the appropriate corrective actions within the States and the various localities.

But it would be in the nature of a multi-agency approach and the lead would be shifting depending on what is the particular problem at issue. If the problem at issue is transportation requirements, the Department of Transportation would take the lead in that regard.

If the problem is law enforcement, then, of course, the FBI would continue to maintain a lead. It would be a coordinated, integrated effort.

Senator **Leahy**. Suppose it turned out that the terrorists captured in this scenario were from a particular group, Iranians, Libyans, whatever, members of an organization in this country which by itself is not a terrorist organization, but is a particular religious or political or social organization for one nationality.

Have considerations been made, or would they be made in such a grave crisis for mass arrests of members of such an organization?

Mr. **Revell**. No, sir; we, of course, do have in this country an infrastructure that does support States that sponsor and use terrorism.

Senator **Leahy**. I know.

Mr. **Revell**. And we do collect intelligence against those that we have reason to believe are directly in support of that terrorist activity. But I would hope that we would never see the day that we would make mass arrests of people because they belong to an ethnic or national group again.

Senator **Leahy**. Again.

Do you compare notes with other countries? I am thinking, for example, if there is any airline that has to be concerned about such threats and receives them fairly regularly, it is El Al.

In Israel, taking off in Tel Aviv or places like that that are a lot closer to the sources of some of these terrorist groups than we are—do we compare notes with them and how they take care of these kinds of threats?

Mr. REVELL. Yes, sir; the FAA has substantial liaison with the counterpart agencies and, of course, we have both security and police exchange with Israel and other allied countries.

We know exactly how the Israeli Government provides protection to El Al. We could do that, too, but it would take the entire Defense Department to do it because that is the level of security that they provide to El Al. Of course, it is a very small operation. We could not even come close with FAA or other non-military capabilities of providing that level of security to U.S. air carriers.

Senator LEAHY. Well, they are also dealing with only, what, two major airports?

Mr. REVELL. Yes, sir.

Senator LEAHY. Mr. Woloshyn, let me ask you this. You have talked about the emergency management systems. How do we make sure that they do not break down? Have you pushed them in some of these games or plans to see whether they would actually break down?

Mr. WOLOSHYN. Yes, in fact, we have. Very recently, we had an opportunity as recent as May of this year to use a system which we developed in FEMA called the IDS, the Information Display System, and the system was very practical and very operational in focusing on a particular part of the country in which there was a particular terrorist incident and identifying the production capabilities, the demographics, identifying the road networks, hospital facilities, and so forth, and it works very well.

Senator LEAHY. Do you include the White House in these games?

Mr. WOLOSHYN. Excuse me?

Senator LEAHY. Is the White House included in these games?

Mr. WOLOSHYN. The White House—we do have in any number of these exercises members from the National Security Council that attend and, of course, the White House is aware of some of the larger games that go on.

Let me also suggest, Mr. Chairman, that we are in the process right now of working with other departments and agencies in identifying information that they may have available which would be useful in emergency management decisionmaking, so that, in essence, we would not be floundering at the time of a particular incident trying to figure out where and how we can get hold of certain information that may be critical.

We would be able to identify immediately those individuals that have certain data bases and can provide them and how we can access that information to help the decisionmakers. So, that is a major item that we are working toward and there is a tremendous amount of interagency support in that regard.

Senator LEAHY. Well, if you get into anything this major, it would go beyond the National Security Council. The President himself is going to have to be involved, would you not assume?

Mr. **Woloshyn**. I am not prepared to make those assumptions, Mr. Chairman.

Senator **Leahy**. All right. I will make them for you.

You talked earlier about sending out information possibly even over the Emergency Broadcast System. Have you discussed among yourselves just to what extent sending out such information using that system itself increases panic?

Mr. **Woloshyn**. I cannot honestly say that I personally have seen information to that regard, but perhaps we have it available some place in the agency. I will be happy to check and provide that for the record.

Senator **Leahy**. Well, I am interested in just what kind of policy guidelines you have regarding informing or advising the public. Are there guidelines to help decide at what point you start telling the public what is happening?

At what point do you say, you know, we caught two people? That is the good news; the bad news is that there are several out there with three more Stingers and we do not know where they are going to hit.

Mr. **Woloshyn**. Let me give you an example, Mr. Chairman, of something which is, in fact, imminent and which we have already undertaken. As you are aware, Cosmo 1900 is a Soviet satellite that may conceivably reenter the earth and does have a radioactive power system.

We have, in fact, been alerting through our regions and various emergency centers in the States—alerting them on a continuing basis as to the status of the satellite. Internally, we have had meetings among agencies to determine how and who and where things may develop.

If, in fact, there is some injury or disaster or damage that may result from the reentry of the satellite, most of the various agencies and messages—in many cases, alerting messages to the public; for example, protective measures to be undertaken; staying indoors, as an example, during a certain point of reentry.

Much of that would have already been prepared and available, and done with a goodly amount of attention to the impact it may have on popular anxiety. But we have been sharing this information and, in fact, CNN recently had an interview concerning that precise issue. We do inform the public.

Of course, if there are highly classified issues, those issues would obviously not be disclosed. But, otherwise, we would be fairly candid in our descriptions.

Senator **Leahy**. Well, let us go to the biological threat.

Mr. **Alderman**. Mr. Chairman, before you do that——

Senator **Leahy**. Yes, Mr. Alderman.

Mr. **Alderman**. Could I just say a couple words here?

Senator **Leahy**. Sure.

Mr. **Alderman**. The effect that we are getting is that the Department of Defense is sitting by watching everybody else prosecute this crisis and, in fact, that would not be the case.

If you will recall, yesterday morning we had what may have been the beginning of an incident which trailed off to be nothing, really, down at the Naval Reserve recruiting station in Richmond.

When that incident first broke, my Department was in contact with the FBI to see if they were going to organize a crisis center so that we could send liaison people to that to provide the interface with whatever the FBI was going to do in this incident. We would have done the same thing very early in the Stinger threat.

A second point: I think our high technology may be one of our strengths in this as well as our weakness. Mindful of the prevalence of television throughout the United States of America and the media's ability to broadcast almost any newsworthy event over this country in a matter of minutes, if not hours, I would submit to you that by the end of the first shootdown everybody in America who has access to a television set would know what a Stinger missile looks like and would have a pretty good idea of the capabilities of it.

It is not a small device; it is not simple to hide. Anybody who wants to stand up in an open field or try to get one in an open field is probably going to be seen. So, the effect would be that you would have expanded your intelligence-collecting net for every man, woman, and child who has access to a television set.

Senator LEAHY. I think that that is a very good point. Of course, also in this scenario the people who may stand up in the field and fire that thing say that they have got a martyr complex and are not really going to worry about getting caught.

What we would want to hope for is that somebody would see somebody loading into the back of a van or whatever something that looked like a Stinger.

Mr. ALDERMAN. Yes.

Senator LEAHY. I also think, though, another problem you are going to have in that is that after the shootdown of the second airliner when you announce that there are three more Stingers out there and you show them the picture of it, you will within a matter of hours have at least a thousand of sightings of those three around the country. Everybody who sees anybody moving a box or crate who looks out of place in their neighborhood is going to call in.

That is not all bad.

Mr. ALDERMAN. That is not all bad at all.

Senator LEAHY. But, also, I think one of the things you are going to have to consider in the planning when you do that is, as Mr. Revell knows from having to—he has spent enough time in law enforcement having to chase down false leads. You are going to have hundreds and hundreds of false leads and somebody is going to have to make the analysis of just how many can be chased down; maybe all of them until you find the right one.

So, that is an advantage in one sense, but I would also submit that if you have somebody who has made this decision to do something this significant and put the kind of cost, effort, and everything else getting into the country, they are going to disperse themselves around this country and they are going to try to cover their tracks very carefully.

I think it would be a difficult situation. What I am concerned about is not just the efforts to apprehend them, but even with the enormous military we have, there is no way that we could try to cover every single place around the country.

What I am concerned about is how our systems continue to work so that you do not have a small handful of terrorists with a handful of not very sophisticated weapons able to paralyze the most powerful nation in the world. That is really what I am addressing.

Obviously, if the FBI or our intelligence agencies or anybody else get information of where these people are, I think we are in a very good position to be able to respond, apprehend them, and stop them.

But in the meantime, before they are apprehended, the damage is not the lives of the 12 people in the commuter plane, tragic as that is, or the 150 or so in the larger airliner, again, as tragic as that is, but the ability to paralyze the most powerful nation in the world, and to have other countries see us possibly paralyzed during that time.

I think of the panic around Rome after the terrorist attack in the Rome airport. I can remember going through that airport not too long after that attack, and seeing some of the bullet holes still in the wall and just being extremely nervous myself just walking through. You can imagine how other people feel. Well, if that sort of thing continues, that is the point I raise.

Let me go to this next scenario because Mr. Revell described an incident involving anthrax in answer to a written question. Let me describe this scenario.

You have a gram of anthrax in a double-sealed ampoule. It is encased in urethane foam. It is found in the offices of a New York newspaper. I will not name the particular newspaper; I will let everybody take credit for it.

But a code name Alpha is used to identify the terrorists, and a typed note says they intend to kill thousands of Americans if their demands are not met. The newspaper immediately informs the FBI; it does not make the information public. The FBI checks it and verifies that it is anthrax spores.

Then TV stations receive broadcast messages from Alpha that it has plans to release anthrax spores in New York City unless certain demands are met. At 8:00 a.m. the next day, Alpha instructs the newspaper to inform the U.S. Government authorities that in a slum building in the South Bronx somewhere they will find a light bulb under pressure and it has one gram of anthrax spores in it.

They say that if their demands are not met, they are going to start riding the subway, go down in the subway and toss light bulbs out of the subway trains. I am told, anyway, that then just the rush of air from the trains would disperse the spores throughout the entire subway system.

They say they will do that unless, again, certain demands are met. Israel has to release all Palestinian prisoners and take other steps which they would not do, nor could we expect them to do.

Then, 24 hours later when Israel has not done this—as, again, we would not expect them to—three light bulbs are thrown from subway trains with anthrax spores in three different sections of the city.

Now, Mr. Revell, you have stated the FBI is currently in the planning stages of a plan for FBI response to chemical-biological terrorism. Before we go into the specific scenario, where do we stand today just on chemical-biological terrorism?

Mr. **Revell**. Well, fortunately, we have never had an incident that has been successfully concluded. We did have a situation back in the early 1970's and late 1960's where a group in Philadelphia attempted to poison the water with a biological agent.

We do indeed see the potential. The Bhopal situation shows the effects that toxic chemicals can have. We realize that no law enforcement agency has the technical ability to deal with the potential of both the biological and chemical threat on their own. So, as in most other situations, we are seeking out throughout the Government those entities that could provide support to the total Federal and State and local effort.

In this particular situation we would, of course, immediately conduct the analysis on both the note and the sample itself through our own facilities. Once we had determined that it was indeed anthrax, both HHS and the United States Army Research Institute for Infectious Diseases, as well as HHS' Centers for Disease Control, would be brought in to participate in this process, as would FEMA, the Department of Transportation, and, of course, the White House itself through the NSC.

There are substantial resources available to the Federal Government. In addition, of course, we are dealing with the largest metropolitan center in the United States and they have substantial resources from the health and emergency services standpoint themselves.

What we would be doing, of course, is attempting to immediately locate the individuals that were carrying out this activity and to preempt their capacity for carrying out any further activities.

At the same time, we would be engaging with the appropriate agencies in contingency planning on a worst-case scenario and being prepared for alternate means of transportation, for panic control, crowd control, and other emergency relief, which would be consequence management, and that would be essentially the responsibility of the other agencies I have mentioned, as well as the State and local authorities in New York.

Senator **Leahy**. In your written answers are some of the things you referred to here today. You discussed an incident in September 1967, when a member of the Revolutionary Action Movement approached an FBI agent and talked about their plans to incite a riot and put cyanide in food and beverages.

Your written response says that you found that RAM had 10½ ounces of cyanide, which is enough to kill at least 45,000 persons. And in another incident you mentioned, in 1972, men in Chicago were planning to contaminate the water supply in Chicago. They were arrested and found to have cultures of typhoid, anthrax, and botulism.

Another example you cited was in 1974, when a man who had threatened to unleash nerve gas in Washington with the intention of killing the President—you found that he did have a nerve agent, as well as explosive devices.

In 1985, the Covenant Sword in the Arm of the Lord was found to have a 55-gallon drum of cyanide, which I understand, depending upon how used, could itself kill enormous numbers of people.

From all this information you provided, I would assume that the scenario I have described—the use of anthrax spores under pressure in a light bulb—is a very feasible thing. Is that correct?

Mr. **Revell**. I am sorry.

Senator **Leahy**. The use of anthrax spores like that——

Mr. **Revell**. Feasible? Yes.

Senator **Leahy**. That is feasible?

Mr. **Revell**. Yes, sir.

Senator **Leahy**. A gram of anthrax—if you were to disperse it, and given some kind of ability to disperse it like this or through ventilation ducts of a major building in the World Trade Towers or something like that—how many people could that much of anthrax kill?

Mr. **Revell**. I do not really know. That is the reason we depend on experts. I do know that the anthrax spore is almost indestructible, and once unleashed it has been known to contaminate an affected area for up to 30 years. It does not take a great deal of it to, one, be lethal and, two, to spread and multiply.

We would, of course, be calling on the expertise of those entities that I have mentioned to tell us the possible extent of the contamination, how it would have to be dealt with, how it would have to be quarantined, what action could be taken to minimize the potential of the spread, and so forth.

Those are areas that neither the FBI nor the New York Police nor any other intelligence agency could really deal with. We would have to be dealing with the Centers for Disease Control and the military research components that have the expertise in this area. They would be providing us with that technical expertise, as well as preparing for consequence management.

Senator **Leahy**. Is anthrax available in the United States, such as in medical laboratories or hospitals or agricultural research facilities?

Mr. **Revell**. Yes, sir.

Senator **Leahy**. In fact, are a number of extremely lethal biological and chemical agents and toxins available in just about any one of these places I have talked about?

Mr. **Revell**. Well, the thing, I think, that would demonstrate that is Bhopal where a chemical plant killed 6,000 people, a fertilizer operation. Obviously, there are extremely toxic chemicals, there are extremely toxic biological agents that are available in the world and can be put to serious use by terrorists, as well as for medical and other research.

Senator **Leahy**. Well, Mr. Alderman has talked about the description of a weapon, in this case a Stinger, and also some of the small SAM's. But in this case with some of the biological weapons that could be used here, it might well not be the FBI, the Department of Defense, FEMA, or DOE, but it might be the Department of Agriculture that might be your best source of information.

I am trying to point out that you do not have to go to some sophisticated, almost James Bond or major military-type facility to get these things, but you are really talking about a fairly open agricultural research center.

Mr. **Revell**. We would look for the best vet in the country, I will tell you that.

Senator **Leahy**. Do you have any kind of a data base on the materials that might be used by terrorists who threaten such mass deaths, or where they might get it?

Mr. **Revell**. Well, what we try and do is not replicate work that has been done elsewhere that would be applicable. As I said, there are a number of military entities that obviously have been concerned with biological and chemical warfare and have done tremendous research in this area.

I would defer to Mr. Alderman, but the United States Army Research Institute on Infectious Diseases is the one that we have turned to for information on such biological agents as anthrax, as well as the Centers for Disease Control under HHS in Atlanta.

Senator **Leahy**. Let me ask a question that occurs—every so often we have an incident—we had one near an embassy recently where terrorists ended up blowing themselves up while setting a bomb—something like that has happened at different times.

Is something like anthrax so sophisticated that a terrorist might not be able to handle it and might end up just infecting themselves? Assuming you have a level of sophistication and training in a terrorist, is this something they could handle? Does anybody know that?

Mr. **Revell**. Well, anthrax is almost always fatal if it is inhaled. It is not necessarily fatal if it is introduced into the body through a cut. So, obviously, there are means in dealing with protecting the respiratory system that if the terrorists are aware of them, they could probably, one, keep it sealed in something like a vacuum bottle or, two, protect themselves with gear.

That, of course, is known to us as well and how to deal with the site of the infestation, as well as dealing with the consequences.

Senator **Leahy**. But if the terrorist is given the anthrax in a properly sealed vacuum bottle of some sort and if they do not care what happens to them at the time they release it, they are pretty much invulnerable, then, unless they are caught.

Mr. **Revell**. It would be very difficult to detect.

Senator **Leahy**. One of the things that comes here, and we have kind of alluded to it in the discussion, for example, in the scenario where the New York newspaper gets the threat. They do not print it; they call the FBI immediately, which I think is a fairly realistic thing. I think the most responsible newspapers would react this way. They would say, hey, look, guys, what have we got here?

Mr. **Revell**. That has happened frequently.

Senator **Leahy**. I know it has. At some point, though, is there a policy that is already spelled out, or does it become a case-by-case basis, when you decide when the information is made public and how much?

This comes into perspective when I think of what happened at Three-Mile Island. The information that came out was not accurate. All kinds of rumors and speculation went on.

A far worse situation was Chernobyl, where the information came, aside from what we were able to determine from our own intelligence people, even from commercial satellites and from detection of radioactivity in some of the Scandinavian countries, as I recall.

Of course, once the panic starts, you are in a difficult thing when you stand up and go on TV and say, well, now we are going to tell you exactly what is going to happen or is happening.

What is the policy?

Mr. **Revell**. Well, as you know, the current Attorney General was the Governor of Pennsylvania during that situation, and one of the things that he was very adamant about is after the initial information that the accurate information be published.

We have gamed situations of very high threat potential to the public and, very frankly, there is a dilemma. If the announcement of a threat is of greater threat to the public's welfare itself than the information being released, the threat from that incident, there is a dilemma and it generally would land on the desk of the President in the scenarios that we have gamed, and under this one I think it would.

There would be advice as to what is the extent of potential loss of life and injury from the agent itself and what is the likelihood of panic and destruction through panic if there is an announcement as to the incident that is uncontained.

The President does have the responsibility to protect the welfare of the public at large, and he would have to make a decision as to which is the greatest risk to the public, the fact that there is a biological agent or the fact of the possible panic that would ensue and how that information was released.

I am quite confident that information would be released. The extent of that information and the timing of it, I think, would be subject to his determination with his advisers as to when the public interest would be best served for that information to be released.

Senator **Leahy**. Well, I ask because I do not know if you have ever taken the subway system in New York City; I have. I could just see being down there in rush hour and somebody says, hey, I was just listening to my radio here and they say they are going to release a deadly organism of some sort, nerve gas, anthrax, whatever, some time during rush hour. I did not hear it all, whether it is today or tomorrow that they are going to do it. Is that not a hell of a thing?

Now, I suspect that there would probably be some consternation in the subway system among the riders, some of whom can be volatile under the best of circumstances. [Laughter.]

You know, it is even conceivable that the message might get distorted by the time it went from one end of the car to the other.

Mr. **Revell**. It is not only conceivable; it is likely.

Senator **Leahy**. I think I would rather be on my farm in Vermont at that point. But you see the point I am making?

Mr. **Revell**. Yes, sir.

Senator **Leahy**. I mean, where do you put the balance between saying, we have got a real threat that we might have a whole lot of deaths in the subway because of the anthrax, compared to how much worse is it going to be if we tell you what might happen, but knowing that there could be nearly uncontrollable panic in those subways?

Mr. **Revell**. In the hypothetical, and I am going to give it to you the way I see it, we would try and get the subway system shut down and cleared before we would make an announcement as to why it was done.

After that was done. I think we would have to come out with a very frank statement that we had a terrorist threat to contaminate the subway system and it was believed to be real, and that the only prudent thing to do was to take precautions.

If we made the announcement as to the threat before the system was secured, I think the consequences would be even worse. Now, that would be my judgment. I would not be making that judgment. It would be made by the governor, the mayor, and the President because you do not shut down the New York City metropolitan system at an operational level; you do that at the policy level.

Senator **Leahy**. There is no question in your mind that something like this does go right up to the President's desk, right up to the governor—using New York as an example, the Governor of New York and the mayor of New York?

Mr. **Revell**. No question about it.

Senator **Leahy**. Again, who coordinates the crisis management at this point?

Mr. **Revell**. The National Security Council apparatus coordinates. We would continue to——

Senator **Leahy**. But they do not have enough people to coordinate something like that, do they?

Mr. **Revell**. Well, they do through the interagency process. I am not talking about the NSC staff. I am talking about the NSC apparatus.

Senator **Leahy**. I see.

Mr. **Revell**. You can essentially bring in the totality of government through this process. But a very important factor here is the fact that the State and local governments are equal partners in this process, and so there it would not just be the Federal Government through the NSC process, but dealing with the governments of both the State and city in dealing with it.

Now, we fortunately have in New York a joint task force on terrorism, so we already have a mechanism to deal with the law enforcement issues. I am certain that that would not be a problem for us, and that law enforcement apparatus gives us direct access to the mayor, to the governor, to the attorney general.

But when it gets into the area of the political ramifications—political in the large sense, the good of the body politic—then obviously the President is going to become involved.

Senator **Leahy**. Well, let me go to an even worse step. Let's say they release the spores in a way calculated to cause maximum dispersal. How does DOD come into this? Do you come in to maintain order?

I am thinking of the way President Johnson sent the 81st Airborne into Detroit during the 1968 riots. I now know exactly what legal questions subsequently came out of that. But if you had this, you would have not only panic, but enormous numbers of deaths and cases of sickness. I would assume that State and local governmental abilities to maintain order would probably be taxed, or even overwhelmed. Does DOD step in?

Mr. **Alderman**. DOD does not step in, per se, until certain things have happened. First, there would be a request from either the mayor of New York or the governor of the State that says this situation is beyond our capabilities to cope with; we need help in the following areas.

That would go through the Attorney General, and probably the decision would be made by the President. And then DOD would come into play with what assets we can bring to bear, again, working for the lead agency in this instance, which would still be the Department of Justice in the way this thing has unfolded.

We do not step in absent a request unless it is a total and catastrophic breakdown of all the infrastructure in the State and there is nobody responsible to say we need help, and then we would only do that at the direction of the President.

Senator **Leahy**. Let me just back off a little bit, then, from terrorism just so I fully understand this. Let us move away from the law enforcement issue. Say there are no terrorists or anything else. Let's say we face the Bhopal type of incident.

Suppose we have just had a catastrophic accident from a medical lab or in the transportation of anthrax or some other lethal agent. There is a terrible accident and we have a Bhopal situation.

Is there either in FEMA or anywhere else a plan to mobilize enormous numbers of medical personnel, medical supplies, trained people, and so on, to step into wherever it might be, whether it is Washington, DC, Burlington, VT, or Casper, WY?

Mr. **Woloshyn**. Mr. Chairman, the first notification that we would receive of that kind of an accident would probably involve immediate notification of all the departments and agencies as to the nature of the accident, including HHS.

Health and Human Services is the lead agency in the development and implementation of a system called the National Disaster Medical System. In essence, what this system would provide is, in the case of a catastrophic disaster which would entail perhaps hundreds of thousands of casualties which would swamp the capabilities of local or State or regional medical services—they would be in a position to call upon other hospitals and other health care providers in other parts of the country to assist in trying to mitigate the injury to the public resulting from that.

So, there is a plan in place. It is a system which has been essentially introduced approximately 2 years ago and it is still in the process of being fully developed, but it is in place and it would be a potential medical capability available to the federal government.

In addition to that, through the Defense Production Act there would be considerable capability available to the Government to allocate priorities in the production of various pharmaceuticals, antibiotics, and so forth, health care supplies, that would be needed.

We would be in a position to, in essence, provide for a continuing supply of what is already in inventory, as well as enhance the productive capabilities of companies to provide for certain materials that may be scarce.

So, yes, the plans are obviously not specifically designed for that particular kind of incident, but the generic response capability for those type of events is either in place or well advanced towards full development.

Senator **Leahy**. Let us turn to the last scenario, if somebody could just stick that up on the wall.

Gentlemen, I realize that in every one of these scenarios you can keep making it worse and worse, which tells us two things, at least as far as I am concerned.

One is that you really have to game these things out because I think that they are realistic possibilities. We all pray and hope that nothing like this ever happens. We hope that between our law enforcement, intelligence, and other organizations, we would catch the terrorists before they even got into our borders. Without going into matters we cannot discuss in an open hearing, we have certainly had some successes along that way, as have other countries that have worked with us.

But I think we have to be frank to say that there probably are no solutions or there are only partial solutions to some of these threats. In some of the areas of panic, there is nothing we are going to be able to do about that, whether the President is speaking directly to the Nation or not.

In some of the things, a disaster could be such that no matter how much FEMA or HHS coordinates or anything else, we completely overwhelm the medical facilities even of a nation as large as ours.

Talking about something that might cause terrible burns, I think in the whole Northeast, we can handle maybe a hundred intensive burn situations at any one time. We could have a situation where a thousand burn cases could need help.

Mr. Badolato, this scenario about our electricity system is going to get into your bailiwick because this could happen both with terrorism or nonterrorism.

In the recent Seattle power outage there was no terrorism involved. Just one junction box has a fire, and a big section of Seattle is closed down for several days. When they went to turn the power back on nobody knew exactly what might happen.

In this scenario, terrorists simultaneously bomb key electricity transformers and switches in the northeastern United States, including the extra-high-voltage transformers—causing a major disruption of electricity.

It is mid-winter; it is well below zero in a number of parts of the Northeast. The electricity demand for heating is near peak. Those terrorists make no demands, no threats, no communication. New York City is especially hard-hit. Traffic lights are out; there are massive traffic jams. We have thousands of cars just abandoned on the streets. I mean, it is so horrible, it is like Washington with 2 inches of snow. [Laughter.]

I am sorry. That is a little Vermont dig.

Back to the scenario. You have got massive traffic jams; cars are abandoned. Everything is just closed up. The nuclear power reactor in the Northeast loses all electrical power. Seven days later, the power loss is still out. Temperatures remain below zero. The natural gas pipeline partially fails because it does not have any power, and after 2 weeks only 35 percent of electricity is restored.

Now, Mr. Badolato, is that a realistic scenario?

Mr. **Badolato**. Yes, sir; even though it is more serious than anything we have faced to date, I would have to say it is plausible.

Senator **Leahy**. I do not want everybody to think that somewhere poised on our border is a group coming down about to do that, but what I am saying is that you could seriously disrupt this amount of electricity by following the steps I laid out here?

Mr. **Badolato**. Mr. Chairman, technically, this is capable of happening.

Senator **Leahy**. All of this, I took out of public material such as books and studies about terrorist threats.

Now, in this scenario the transformers are bombed. Let us just take it down step by step. Who assesses the damage and begins to coordinate the Federal Government response?

Mr. **Badolato**. Well, the first thing that would happen, because of the severity of this particular situation and the speed of things happening in the electric world, we would be immediately aware of this through our emergency contacts with the industry, which itself has to take immediate actions.

But both Federal and State Government emergency organizations would be aware that industry had tremendous problems and was taking immediate actions. Immediate activities by the industry would include such things as local load curtailment plans, damage assessment and reconstitution planning, et cetera, the type of things that the electric power industry is capable of doing swiftly even in a very, very serious catastrophe such as this.

Within the Federal Government, we would be working principally on the industry side with the North American Electric Reliability Council. They have a hot line to all of their member utilities around the country and would be able to help us and provide us with assessments of local and regional impacts.

At the same time, we have other contacts within industry through the emergency electric power section of the National Defense Executive Reserve Program. We know these individuals extremely well, particularly in the region cited in your scenario. We have met and have participated in crisis management exercises and simulations with the heads of the Northeast Power Coordinating Council and the New York Power Pool at least a half a dozen times. We would be in contact with these individuals, as well as NERC.

We would also utilize the Department of Energy's communication system with each of the State energy offices. That is an electronic mail system we would use to transmit to the States what we understand is going on and working back and forth to coordinate the response.

Senator **Leahy**. The communications system would keep on working even though you are having enormous power outages?

Mr. **Badolato**. We understand that there may be some degradation, but we think we could work through that. If that failed to work, we would go immediately to FEMA and get their assistance and access to their emergency communications system. We plan on doing this and we are not going to fumble around too much in establishing communications with the States.

Simultaneously, the industry will be doing a lot for itself, as the principal member of the triad of industry, the Federal Government, and the States working together to assess the situation and coordinate their response.

Industry will be working under the auspices of NERC, the North American Electric Reliability Council, which was founded after the

New York City blackout to ensure that things like this did not happen, and if they did happen, that operating procedures were in place and instituted within the electric power industry.

Inside the Department of Energy, let me speak first about what we would do as the lead agency in an energy emergency. We would immediately institute our energy emergency management system, which is composed of a team of experts from each of the relevant sections within the department. The Energy Emergency Management Team [EEMT] would meet immediately to begin an assessment and a situation analysis of what the problem is, and to make recommendations to the Secretary, possibly even the President, on immediate actions which should be taken.

Senator LEAHY. Who is it that determines the priorities as far as who gets what share of the remaining power we have?

Mr. BADOLATO. Well, there are two levels of that I would like to talk to. First, at the State level, we have the States. Each of the public utility commissions require each of the electric utilities to have a load curtailment plan. This is a plan for determining who gets electric power when you only have a limited amount of it; and it is essentially oriented toward health, safety, security, hospitals, police, firemen, and so forth. If there is just a limited amount of electricity, these are the groups that keep things functioning.

Senator LEAHY. They go first?

Mr. BADOLATO. They would come first; this is a civilian-oriented plan down——

Senator LEAHY. Who is second?

Mr. BADOLATO. Well, the relative priorities generally address residential customers, industries, refrigeration, meat-packing, and things of this nature.

It has been our experience in dealing with industry—and, Mr. Chairman, I will tell you we really worked on this very hard in simulations and games, that we do not get a 100-percent blackout in an area; we get islands of power which would be used to build up and spread out the restoration of service.

Even though we might agree that there is a very small chance of such an event, we have examined its implications. We have found, particularly in the case of the New York metropolitan area, that in a day or two it would be likely that these islands of power would be identified and would begin moving out within a week or two, and I would say 35 percent service restoration is probably fairly realistic within a couple of weeks.

So, power would be returning gradually. We would be concerned about emergency power to drive such things as the banking industry and other computer-driven industries. Emergency power, portable generators and things of that nature would be in tremendous demand.

Senator LEAHY. Do you have a data base for different areas around the country so you can tell pretty quickly who has got emergency power capabilities and who does not? Again, I remember that Northeast blackout and the pilot saying he was amazed when all of a sudden La Guardia Airport disappeared. All the lights went off and everybody assumed, of course, that some automatic generator would throw it right back on, and nothing did.

Mr. BADOLATO. Yes, sir.

Senator **Leahy**. Fortunately, it was a very clear night. I remember I tried three times to land at La Guardia the night before and it was a terribly foggy night. Fortunately, that did not happen the night of the blackout. People got out of there.

But, can you say these places, these hospitals, these banks, these whatever, have a generator, they have a 4-day supply, a 2-day supply, a 5-day supply of fuel, or whatever?

Mr. **Badolato**. No, sir, we at the Federal level do not. We expect that local government and electric power utilities will plan for this and will have worked it into their curtailment plans.

Senator **Leahy**. Have you ever gamed it out and had somebody say, wait a minute, we do not even know how many hospitals have emergency power?

Mr. **Badolato**. We have not had that happen, sir. The utility people have told us that most hospitals in their service area have backup power. In addition, the manager of the local utility has a load curtailment plan which he has had to previously submit or have coordinated with a public utility commissioner or public service commissioner.

This information exists and is a matter of record. We are not aware of the depth of detail there. We have not gotten, say, a "we really do not know" from these chaps.

Senator **Leahy**. Well, that is my point, because I was surprised to see, for example, how vulnerable some of these generators are; again, this is to some extent the price you pay for an open society. You and I would agree it is a worthwhile price to pay, but I am also wondering what you do to be prepared.

Do we have backup generators that can be flown into an area, or does industry as a whole stockpile replacement generators? If, for example, we had a number of major extra-high-voltage transformers that were destroyed, do we have to build new ones before they can be replaced, or can we go to the damaged site and say to the local people here is another one, plug it back in?

Mr. **Badolato**. Well, that is a good point, sir. Inside the Department of Energy our energy emergency management system and team will be working to facilitate some things over which we really do not have direct control, like the generators.

We chair an interagency group on energy vulnerability which meets regularly and whose membership includes the representatives from principal agencies—the FBI, FEMA, DOD, Transportation, and so forth—at the assistant secretarial level.

If, in fact, there was a crisis requiring generators, we do not have such a stockpile in the Department of Energy.

Senator **Leahy**. That is my question. If No. 1, 4, and 5 extra-high-voltage transformers in whatever grid get blown out, what you are saying is nobody can go either in the Government, Federal, State, or in private industry and say here is where we have got another one stored; we can put it in.

Mr. **Badolato**. Well, I was talking about generators. The transformers are a special case, and let me address that, sir, if I could.

Senator **Leahy**. I am told that this is a vulnerability. If it is attacks that are being made, not a malfunction, but actually major segments destroyed, we may not have any replacements that we can move in quickly; that we might be in a position of having to try to build them in a hurry. Is that right?

Mr. **Badolato**. Well, sir, not quite. First, the electric power utilities do have some spares. The problem is that if we have a large attack, a multi-site attack, the spares may be inadequate for the numbers which are required.

Second, these are very large, some weighing up to 500 tons, difficult-to-transport pieces of equipment. Merely to take an old one out and replace it with a new one, I have been told in my visits to industry sites—to prepare it on site, tune it, and get it going again can take several weeks. So, consequently, it is not just a switch-on switch-off type of operation. It is a very large, complex, heavy industry operation.

In the third place, these transformers are long-lead items. It is the current nature of industry to take approximately 18 months to build and get them off the assembly line. Additionally, because so much of the industry has gone offshore, we really do not have an assurance that we can influence production line priorities.

Senator **Leahy**. Mr. Badolato, I think I have some other questions on this, but I think I may save them for a closed session.

Mr. **Badolato**. Yes, sir.

Senator **Leahy**. What about a nuclear power reactor losing electrical power? Are there backup systems so that they do not have to rely on relatively vulnerable transmission lines?

I do not know how anybody makes a transmission line coming into a reactor invulnerable. If they do go out, what about the cooling pumps there? Do they have adequate backup if they suddenly lose power coming in?

Mr. **Badolato**. Yes, sir; the answer to your question specifically is that if a nuclear power plant becomes isolated from the grid, the reactor is shut down. That is standard operating procedure [SOP]. The emergency diesel generators would start immediately and provide power to the pumps which must circulate cooling water as part of the safe shut-down process. Our concern would be, naturally, on the resupply of diesel fuel for the emergency generators until either the unit was sufficiently cooled, or commercial power was restored.

There are a tremendous amount of safety precautions built into the safety guidelines and rules which are in effect. If you would care to go into the details of that, I have somebody who is an expert on the emergency operations of our nuclear facilities here with us today.

Senator **Leahy**. I think I may hold that for a followup question. Natural gas lines—is that also a significant concern? If electricity goes out, are we also facing a vulnerability on our natural gas lines?

Mr. **Badolato**. With natural gas lines, they generally operate on natural gas, meaning that their compressors are, for the most part, gas-driven. However, the importance here of electricity is for the automatic controls provided by computers which govern shunting, pumping controls, and other directions which are given.

Losing electricity would mean that we would seriously impair or impede the transportation of natural gas. Our real problems in natural gas would come from not being able to control its transmission and distribution as effectively as before, especially in winter months.

Senator LEAHY. I promised a couple of the witnesses that I would keep them on schedule. I have dozens of other questions which I may submit in writing, but let me just ask a couple in conclusion here.

Mr. Alderman, you mentioned in both your testimony and in answer to one of my questions something about special operations forces being used in domestic crises. Without going into specific instances where they may have been standing by, you did say this would be a very rare and extreme circumstance?

Mr. ALDERMAN. Yes, sir.

Senator LEAHY. I have met with some of the special operations forces and discussed some of these things with them. I think all of us always get concerned, as I am sure you do, if the military is suddenly brought in to do what might be seen as a law enforcement or a military operation within the United States. For the record, can you tell me how and when, under what circumstances, under what authority, and with what powers special operations forces would be used in a terrorist incident in the United States?

Mr. ALDERMAN. Special operations forces are, first of all, military forces, and so exactly the same authorities and powers that apply across the board to all DOD forces would apply to special operations forces.

They just happen to be military forces with unique and, by definition, special capabilities that are not possessed by the broad body of the Department of Defense's three military services.

These capabilities are tailored to counterterrorist operations externally. They probably would be used at the request of the authorities, the civil authorities, to assist the civil authorities in instances where the conventional force capabilities would not serve to resolve the particular issue. That is about as close as I think I can come to what you are saying.

Senator LEAHY. If military assistance was requested by civil authorities, who makes the decision within the Federal Government to respond to that request?

Mr. ALDERMAN. The Attorney General takes that recommendation or that request, then, with his recommendation, to the President and the President makes that decision, sir.

Senator LEAHY. Now, the special operations military in that situation do not have any law enforcement authority or powers? I mean, they have nothing beyond—I am talking about their legal authority and power—nothing beyond what anybody else in the military would have?

Mr. ALDERMAN. Correct.

Senator LEAHY. There would have been circumstances where they would be deputized in any fashion as law enforcement officers?

Mr. ALDERMAN. I cannot answer that as far as the deputization goes.

Mr. REVELL. Yes; I have right here the Executive order that the President signed on November 24, 1987, providing for the restoration of law and order in the State of Georgia. This was our request, the FBI to the Attorney General to the Secretary of Defense to the President, to augment our capability to resolve the riot in Atlanta.

Military forces were dispatched, specific ones that had specific capabilities, to supplement our tactical teams and to provide us with assistance that, because we had two crises going, Oakdale and Atlanta, exceeded our capability.

It worked extremely well. The military came in and assumed their support responsibility right on line. There were no questions as to the lines of authority, the lines of responsibility. They were, in fact, deputized under the overall leadership of the special agent in charge at the scene, the FBI agent in charge, to carry out certain responsibilities. There were rules of engagement established approved by the Attorney General and the Secretary of Defense.

So, in addition to having gone through a number of these exercises, including the Olympics and Pan Am Games, and so forth, we do have an actual, real situation where it has worked extremely well.

Senator LEAHY. Who was the ultimate commander in that case? Would it be the FBI?

Mr. REVELL. Yes, sir; although the military components were always under the command of their military leadership, but he operated under the direction of the SAC.

Senator LEAHY. That is what I am saying. I mean, you say they were deputized. They were deputized as law enforcement officers?

Mr. REVELL. Yes, sir.

Mr. ALDERMAN. I would point out that these were special operation elements because they had capabilities that were not extant through the rest of the armed forces.

Senator LEAHY. I understand, Mr. Revell, but suppose in a hypothetical situation the commanding military officer there says I intend to send my special forces to do this, this, and this. The ranking Federal law enforcement officer there says no, you will not. The ranking law enforcement officer then wins out in that case, is that correct?

Mr. ALDERMAN. That is correct.

Mr. REVELL. The military officer tells him what he can do and how he would do it. It is up to the agent in charge to either accept that, ask him to modify it. There will always be agreement as to how the military forces will be deployed. Their tactics will be under the control and direction of the senior——

Senator LEAHY. They cannot take an action that has not been approved?

Mr. REVELL. Correct.

Senator LEAHY. The FBI, in turn, may ask them to do something and they might say we just cannot do it.

Mr. REVELL. That is correct.

Senator LEAHY. But on the other hand, they cannot go and take an action when the trained law enforcement officer says you cannot do that under the Constitution; you cannot do it legally, or it just does not fit in with our law enforcement plans?

Mr. REVELL. Only in the case of a declaration of martial law would they have that authority.

Senator LEAHY. One of the feelings I had—and I came to this after 8 years on the Intelligence Committee and 10 years here—is that there have not been successful terrorist attacks in the United States in this decade because terrorists are deterred by our counterterrorist capabilities, which I think have improved.

Would you agree with that, Mr. Revell?

Mr. **Revell**. Absolutely; I have been making that point over and over. [Laughter.]

Senator **Leahy**. Well, I think it is true. I think it has improved and I think if anybody wants to back off trying to improve, they should talk to some of our NATO counterparts in Germany or Italy or France, and ask them what they have put up against terrorism. I think that you will come back here being rededicated, if you were not already, to constantly improving it.

In fact, that is one of the reasons for holding this hearing. It is not so much to ask how many people we have in the special forces or in the FBI counterterrorist units or in our other intelligence agencies, but rather to increase public awareness that we are prepared and preparing to defend ourselves effectively.

I think that making it clear to the rest of the world that the United States does intend to defend itself very effectively in counterterrorism, I think this itself has to have a deterrent effect.

Do you agree with that?

Mr. **Revell**. Yes, sir, I do, and I think that there should be some comfort in the fact that the Government agencies and entities not only at the Federal, but at the State and local level, do come together with a common mission, common purpose, and work very effectively to counter this type of threat, and have done so successfully now for many years.

Senator **Leahy**. One last comment, and I will make it more as a comment than a question because it is something I have discussed with you before and I have discussed it with Judge Sessions and, before him, with Judge Webster. I have certainly discussed it with Secretary Carlucci and Secretary Weinberger before him.

You said in your statement you intend to protect constitutional rights, no matter what the temptation might be to do otherwise, when you are dealing with terrorists. It goes way beyond dealing with a bank robber or something of that nature.

I cannot emphasize enough how important that is. I think that if a terrorist incident were such that it led us to set aside our Constitution, then a handful of terrorists have accomplished what all of the armies arrayed against us in two world wars were unable to do.

That may well be a difficult thing to tell people when they are facing a grave terrorist threat. I remember sometimes how difficult it was for me to tell people this very thing when I was a prosecutor, but it is true.

In fact, a terrorist threat could be designed just to see if they could drive the United States to set aside the foundation of our Government for 200 years. That may sound like a history lesson or a constitutional lesson, and I suppose to some extent it is, but I was glad to hear your reaffirmation. I have been very pleased to hear the same from Judge Webster, Judge Sessions, Mr. Carlucci, and others.

Gentlemen, I appreciate your being here today. I think you have helped raise our consciousness in this. I know we have sent you a lot of material, and I want to extend my appreciation to the Department of Defense, the Department of Justice, the Department of Energy, and FEMA for all of your help in working with my staff in preparing this hearing.

Thank you.

[Whereupon, at 11:28 a.m., the subcommittee was adjourned.]

○